IRIE
International Review of Information Ethics ISSN 1614-1687

Vol. 22 (12/2014)

Ethics for the Internet of Things

edited by Hektor Haarkötter and Felix Weil

Editor of this issue:

Prof. Dr. Hektor Haarkötter

Professor, University of Applied Sciences for Media, Communication and Business
Berlin, Germany
Email: h.haarkoetter@hmkw.de

Dr. Felix Weil

Managing Partner of QUIBIQ GmbH
Stuttgart, Germany
Email: felix.weil@quibiq.de

Editors of IRIE

Vol. 22 (12/2014)

Content:

  ISSN 1614-1687

Editorial: On IRIE Vol. 22

Many science fiction phantasies already claimed that one day machines will be superior to human beings and computers will finally take over. But unlike in Stanley Kubrick's '2001' or Asimow's 'I, Robot' the latest developments in the Internet of Things (IoT) give reason to suggest that if this will happen it won't be necessarily machines that physically resemble human beings with legs, bodies, voices etc. that will do the job (robots in the classical sense). If, then it will be more like in Matrix – the physicality of the necessary intelligence (i.e. computing power) will vanish as it will be incorporated into the physical world of our daily life itself. It won't be separate machine entities that will dominate the human kind but it will be by the embedding of computing power into the ordinary things of our daily life and their being connected with each other to form a virtual pervaded living space. A living space that then could not only be paradise (optimized by the computing power embedded to the best for mankind) or hell (used to encage and enslave its inhabitants) but even more also a pure illusion (encaged and enslaved inhabitants that are made believe and even sense realistically that they are in paradise).

This is what philosophically the Internet of Things is all about: Things won't be physical things anymore that are independent objects for the examination, exploration and manipulation of an equally independent subject. Things will be what is presented to the subject and the subject is what the computed presentation presupposes 'on the other side': a user, a monitored, a … . Thus, if the things change in the IoT we will change. And thus, the underlying philosophical subject-object paradigm has to change as well taking this interplay into account. Again, not only theoretically (as depicted in science fiction far from any possible reality) but very practically regarding our daily life: how we automate our homes, how we care for elder people, the way we monitor our children, the concepts we use to organize life in (smart) cities etc. For the good (of who), for the bad (according to what norm)? This is the ethical challenge raised by the IoT and this issue presents some very interesting answers to it and where not complete answers yet very helpful outlines for possible answers an 'Ethics for the IoT' can give and must give (rather sooner than later).

Yours,

the editors.

ISSN 1614-1687

Felix Weil, Hektor Haarkötter:

Ethics for the Internet of Things

The Internet of Things (IoT) though being the latest major development in the digital sphere already has its own history. It was already in the early 1990s that Mark Weiser introduced the very idea of computing power embedded into entities in the physical world under his notion of Ubiquitous Computing.[1] Later it was also discussed with slight modifications under the concepts of Pervasive Computing or Ambient Intelligence.

In 2007 IRIE has published an issue with the title: "Ethical Challenges of Ubiquitous Computing", edited by David Phillips and Klaus Wiegerling probing "the practices, ideologies, and power relations" of a "mesosphere saturated by information and communication technologies (ICT)"[2]. However, the very concept of an Internet of Things was originally proposed by Kevin Ashton in 1999 during a presentation at Procter & Gamble in order to address the advent of the RFID technology making ordinary things seamlessly identifiable for remote computation. But it is only now after the huge enlargement of the IP address space by ip6 and the further unabated rapid decline in costs of micro processing power that brings together the concepts of Ashton and Weiser to what we are willing to call now the very Internet of Things. This is fundamentally different to the idea associated with both approaches in particular but yet not less revolutionary. It is less the fact that computers today are embedded in more and more everyday items – from cars over mobile phones to TVs – that forms the IoT and thus the subject of this issue. And it is also not the remote computability of distinct physical (RFID tagged) items. The IoT is rather *the being connected of embedded computing capability in finally everything* that will form a more and more coherent digitally coined environment of our daily life.

In the course of the formation of the IoT our everyday world will thus become mantled and controlled by the capabilities of computers *being embedded and connected to each other*: our perceptions and actions, at all-time and everywhere, shall thus undergo some kind of ICT support. Everyday items will consequently not only be eyes and ears for computers but computers will also be connected to these everyday items resulting in hands of computers: billions of eyes, ears and hands to execute actions computers have decided upon which again are seen, heard and measured by other computers leading to further computed actions … – thus, finally resulting in a Creative Circle (Varela) leading not to a new but separate (digital) sphere like the Internet of Websites (with a button to be switched of on every accessing device) but a complete new dimension of our existing physical world (that can't be switched of and thus be treated separately anymore as there is no distinct accessing device anymore): The very idea of an Internet of Things means an omnipresent ICT pervasion and accompaniment of our daily life, either as an active user, as a passive beneficiary, as a monitored and possibly even as a system guided being.

Basically, the IoT will consist of

- perception technology (sensors etc.) embedded in physical entities,
- networks for exchanging the data generated by these,
- computing power for interpreting this very very big data (in real time, as a service)
- and finally agents that react according to the computed results – the latter again embedded into everyday physical items being connected by the networks named above.

According to the research institution Gartner by 2020 more than 26 billion devices will be interconnected in this way – a multiple of human beings on the planet now and then. In a certain sense, our everyday world will be then made intelligent by the capabilities of computing power distributed and embedded into everyday objects and the connectivity of the net.

1 Weiser, Mark (1991): The Computer of the 21st Century. Scientific American 265 (3) 1991

2 Phillips, David and Wiegerling, Klaus (2007): Introduction to IRIE Vol. 8. International Review for Information Ethics 8 (4) 2007

ISSN 1614-1687

There is no question that any technology that is going to so radically encroach on our daily life is in need of a robust ethical framework. Nevertheless, any ethical discussion of the Internet of Things rests inherently speculative because we are dealing with still emergent technology. We therefore have to take into account its full potential, irrespective of how far this potential can or will be realized in detail, and irrespective of the fields in which all-pervasive ICT accompaniment will find acceptance.

This brings into sharper focus two fundamental problems in theoretical ethics that have already attained a special position in applied media ethics in general and are now even more pressing in the IoT: On the one hand, the determination of reality which we should interpret for our moral decisions and which we should influence with our resulting acting. And on the other hand, the determination of the subject to which these actions should be attributed to and that should intervene with this reality. In the IoT we may say that on the one hand reality diminishes with respect to its (physical) confrontational character, and hence becomes more and more if not completely virtual or at least intrinsically virtually determined. The reality in the IoT won't be a sensational re-presentation of the physical world but more a virtual presentation involving and mantling it – intrinsically physical and virtual at the same time to different degrees and extents in different situations which won't necessarily be transparent to the subjects involved.

And there comes into focus the subject that is perceived by intelligent systems always as a user stereotype, i.e. as a buying, sick or travelling subject etc. In a certain sense the subject in the IoT becomes weakened to the extent that some are willing to deny moral agency to the then computer enhanced/guided/discharged human beings and others are ready to ascribe moral agency not only to them alone but also to robots and computers interacting in the IoT; finally two ends of the same discussion. Yet, the status of the various agents in this virtual and interwoven reality is still to be clarified either regarding their moral accountability themselves (its degree like with adolescent human beings?) as well as its delegability (like from the product to its producer?).

Yet, looking deeper into the underlying developments it is not only the subject in certain situations but also its formation, the formation of its identity that is fundamentally affected by the IoT. This is because it has to above all manufacture its personality without the recognition and non-recognition of a present other genuine subject free of digital enhancement, and possibly without the development of those specific skills dependent on this confrontational experience of the 'naked' world and the 'naked' other. Our everyday respective abilities end up becoming substituted or at least adjusted by the intelligent systems underpinning it.

Thus, the experience of the world and the self will undergo a fundamental transformation in the IoT. At the possible end of this development it can happen what Ashton called the independence of the internet from any human intervention. The role models of active or passive participation in world affairs could then change dramatically, and the ethical dimensions of this transformation affect human actors as much as the "things". Most interestingly, the old English and German word "thing" etymologically meant a public assembly and therefore was a synonym of democracy and partizipation. The "Internet of Things" on the contrary will possibly become a notion of usurpation and the domination of computers over their former creators.

While this apocalyptic scenario portrayed in science fiction like 'Matrix' is to be considered as an extreme potential one thing remains for sure: things in cyber-physical systems - i.e. in the IoT, i.e. in our future everyday world - won't remain the same as in pure physical reality today and thus we won't remain the same either as the relationship to the world is constitutive for the subject. What (sic!) things will be in the IoT and how our self-understanding has to change accordingly is the very question at the bottom of any possible ethics for the IoT.

Questions to be asked; to be re-thought

A possible and urgently necessary ethics for the phenomenon of an IoT is anchored in the field of information ethics, yet it radicalizes the fundamental issues in this area, insofar as the entire mesosphere appears as a sphere pervaded shaped and (in-)formed by virtual/computational facticities. Thus major issues of any ethics for the IoT are all yet addressed by infoethics but must be re-formulated and re-thought in the light of the above described radical developments:

Privacy in the IoT

Of course, a major issue of the Internet of Things is privacy. As our everyday life will be invaded by sensors that are connected to computing power to process the 'Big Data' gathered the unprecedented possibilities to breach privacy are easily predictable. But again in the IoT the quest for privacy is radicalized to the extent that the blurring of the contexts that define the realm of privacy and the public demands new fundamental concepts to define what these notions can really mean in the Internet of Things.

Access to beneficial use of IoT and social justice

Assuming that access to the Internet of Things is beneficiary for people and given its pervasiveness the potential making use of it may become a fundamental human right and constitutional for personal development. What do we have to do to avoid respective impairments and divides?

Establishment of trust in the IoT

The more our everyday life becomes dependent on the technologies deployed in the IoT the more a framework is necessary to ethically establish trust in the IoT. How can we and should we enable subjects to take informed decisions on attributing or depriving trust into the machinery.

Status of agents and agency in the IoT

In the case of the Internet of Things it is vital to clarify whether things that can act enabled by connected computing power are also actors from an ethical point of view. Can these things be attributed to some form of responsibility or accountability or only their originators? And how to regulate that?

Answers given or outlined by the contributions of this issue

The above named fundamental questions are explored by the contributions of this issue in different ways and dimensions:

- **Ori Freiman** asks if the concept of trust can provide a possible framework for constituting moral interaction in the IoT: Do we have to embed structures of trust into the things and their relationships as efficiently as we are embedding computing power into these? And how could this be achieved?
- **Caroline Rizza and Laura Draetta** are more sceptical regarding "technocratic approaches" to an ethics for the IoT. They argue, "that only human agency and user empowerment constitute a valid answer to the ethical, legal and social issues raised by IoT" and therefore demand a fundamental right to "silence the chips of IoT-things".
- **Soenke Zehle** is exploring a middle course by not opting for either silencing or unrestricted humming but proposing 'Depletion Design' as a fundamental design strategy to 'reclaim the ambient commons' in the IoT. "The idea of depletion design is … to establish an experimental institutional object to facilitate and frame such ethico-aesthetic practice, an architecture for commoning that situates and affirms our ethical agency under the conditions of mediation."
- In their contribution **Roba Abbas, Katina and M.G. Michael** look more specific into the challenges Location-Based-Services are rising. It is a very comprehensive review of the respective techniques, their social application and the ethical challenges implicated. The authors finally propose a "socio-ethical conceptual framework" to address the fact that in the IoT "for the greater part, the human is removed from decision-making processes and is instead subject to a machine."
- **Sandrina Dimitrijevic** elaborates on the "Ethical Consequences of Bounded Rationality in the Internet of Things". She argues that any possible ethics for the IoT has to take into account that rationality in

the IoT is by default bounded and we therefore cannot rely on informed consent alone as a last authority e.g. regarding privacy and giving away one's own data.

- **Kashif Habib** addresses the "Ethical Aspects of the Internet of Things in eHealth". While in his eyes "the healthcare system can get many benefits from the IoT such as patient monitoring with chronic disease, monitoring of elderly people … [this] comfort may bring along some worries in the form of people's concerns such as right or wrong actions by things, unauthorised tracking, illegal monitoring, trust relationship, safety, and security." His paper presents the respective "ethical implications on people and society, and more specifically discusses the ethical issues that may arise due to distinguishing characteristics of the IoT."
- **Bernhard Stengel** presents "Ethical Thoughts Regarding Smart Homes". He also holds that smart technology may be more efficient than human beings in optimizing e.g. energy consumption but is also concerned about the underlying paternalism. What are the underlying norms for the optimization executed by these very efficient home automation systems?
- **Burkhard Schafer** sees "Data disposal as a challenge for waste management in the Internet of Things". The IoT will not only produce masses of e-waste we have to deal with in future but also d-waste: data stored on the billions of devices giving account of the everyday life of their users also and even more when disposed. Therefore, Schafer concludes: "Operators of large recycling schemes may find themselves inadvertently and unknowingly to be data controller for the purpose of Data Protection law, private resale of electronic devices can expose the prior owner to significant privacy risks."

Ori Freiman:

Towards the Epistemology of the Internet of Things

Techno-Epistemology and Ethical Considerations Through the Prism of Trust

Abstract:

This paper discusses the epistemology of the Internet of Things [IoT] by focusing on the topic of trust. It presents various frameworks of trust, and argues that the ethical framework of trust is what constitutes our responsibility to reveal desired norms and standards and embed them in other frameworks of trust. The first section briefly presents the IoT and scrutinizes the scarce philosophical work that has been done on this subject so far. The second section suggests that the field of epistemology is not sufficiently capable of dealing with technologies, and presents a possible solution to this problem. It is argued that knowledge is not only social phenomena, but also a technological one, and that in order to address epistemological issues in technology, we need to carefully depart from traditional epistemic analysis and form a new approach that is technological (termed here *Techno-Epistemology*). The third and fourth sections engage in an epistemic analysis of trust by dividing it in to various frameworks. The last section argues that these various frameworks of trust can be understood to form a trustworthy large-scale socio-technological system, emphasizing the place of ethical trust as constituting our commitment to give proper accounts for all of the other frameworks.

Agenda:

ISSN 1614-1687

Author:

Ori Freiman

- Ph.D. Candidate, The Graduate Program in Science, Technology and Society, Bar-Ilan University, Ramat-Gan, Israel
- ✉ freimano@post.bgu.ac.il

Acknowledgments:

I thank Boaz Miller, Michelle Spektor, Talia Fried, Michael Eldred, Felix Weil and two anonymous reviewers for their useful comments and suggestions.

This paper discusses the epistemology of the Internet of Things [IoT] by focusing on the topic of trust. It presents various frameworks of trust, and argues that the ethical framework of trust is what constitutes our responsibility to reveal desired norms and standards and embed them in other frameworks of trust. The structure of the article is as follows: The first section briefly presents the IoT and scrutinizes the scarce philosophical work that has been done on this subject so far. More generally, I argue that an adequate epistemic theoretical framework that deals with technology has not yet been developed. The second section suggests that the field of epistemology is not sufficiently capable of dealing with technologies, and presents a possible solution to this problem. I argue that in order to address epistemological issues in technology, we need to carefully depart from traditional epistemic analysis and form a new approach that is technological (termed here *Techno-Epistemology*). The third and fourth sections engage in an epistemic analysis of the concept of trust by dividing it in to various frameworks (referred to here as layers). The last section argues that these various layers of trust can be understood to form a trustworthy large-scale socio-technological system [LSSTS], emphasizing the place of ethical trust as constituting our commitment to give proper accounts for all of the other layers.

More specifically, the second section introduces individual epistemology's quest for justification in order to acquire knowledge, and its relatively recent development of social analysis. Building upon Paul Humphreys' (2009) framework of *Network Epistemology*, this section criticizes both individual and social epistemology for being anthropocentric, and argues that this renders individual and social epistemology unsuitable for a proper epistemic analysis of technology. An alternative framework to traditional epistemic analysis, namely *Techno-Epistemology*, is introduced and applied to the IoT. By presenting the concept of *Scientific Instruments of Things* [SIoT], a hybrid view of scientific knowledge generation and distribution, for both human and non-human epistemic agents and their related social and technological processes, is suggested. Epistemic differences between networks of humans and machines are highlighted in order to raise a dual question of trust: how will humans trust the network of the IoT, and how can justified relations of trust form between scientists and the SIoT?

The third section deals with various layers of trust. Beginning with the *trust-reliance* distinction, the fundamental question of whether or not trust relationships between humans (as moral agents) and non-humans (as non-moral agents) are possible, is discussed. McDowell's (2002) distinction between *epistemic trust* and *social trust* is presented, and Lehrer's (1995) and Sosa's (2006) accounts of trust are offered in order for human users and scientists to epistemically trust the IoT and the SIoT. Next, the ethical dimension of trust is identified as the "unseen link" between epistemic trustworthiness and norms and standards. I argue that norms and standards should be the focal-points in trust formation. A recent discussion about the topic of trust in the context of the IoT (Kounelis *et al*. 2014) and Nickel's (2013) *Entitlement Account,* which addresses direct trust in artifacts, are brought forward as examples for social processes that can set the technological norms and standards, and also as a suggestion of the formation of social trust in the context of technology and knowledge.

The fourth section discusses *techno-trust*[1] between IoT devices. As a general example, I suggest the formation of a reputation system for the IoT and SIoT devices. This system will not only present evidence for trustworthiness for these devices, but will also form a rational basis of trust for human users of the IoT and SIoT. The main argument is twofold, and normative: A) An adequate theoretical systematic epistemic framework that analyses technology must be developed, and B) The ethical layer of trust is what constitutes our responsibility to reveal desired norms and standards and embed them in other frameworks of trust in order to form a trustworthy LSSTS.

[1] For methodological reasons epistemological concepts are distinguished from those of the Techno-Epistemological framework by the prefix "techno-".

A Lack of an Adequate Epistemic Framework for Analyzing the IoT

The IoT is one of the most popular technology-buzzwords, and with good reason. As an infrastructure upon which many applications and services function, the IoT is based on the idea of connectivity, for any thing, any place, and any time. It represents real-world objects that are connected in a network, continuously sensing, collecting, processing and communicating. When it is joined with technologies that enable ultra-fast connection, and that of cloud computing (the idea of providing centralized computer-related services), vast amounts of storage memory and processing power are available to the clients – whether they are humans or machines[2]. The idea is not only to transmit live data, for example, the heart rate of a patient to her doctor, but to be able to correlate real-time potential events with similarities, correlations, and abnormalities present in the "big data" that were processed and mediated through many IoT devices[3]. While the IoT's sensors "act as the digital nerves for connected devices, the cloud can be seen as the brain to improve decision-making and optimization for internet-connected actions related to these devices" (van den Dam 2013).

As technology and technological solutions advance over time, the overlap and convergence between various fields of applications (and studies) increase. The IoT represents this kind of convergence and overlap (together with cloud computing and ultra-fast broadband network connectivity, as mentioned, among other infrastructure technologies) by increasing the amount and sophistication of sensing, processing, and communicating, ultimately enabling us to create knowledge from the vast amounts of collected real-world measurements (Stankovic 2014). These technologies already have many applications and its potential applications reach all areas of life (for many examples, see ERCIT 2012 and references within). The IoT devices are estimated to soon become the largest device market in the world[4]. However, the realm of philosophy still has not provided an epistemic account for the IoT.

By the same token, an epistemic theory within the Anglo-American analytic philosophical traditions, which deals with technology in general, has also not yet been developed[5]. Such a theory would ultimately enable reflections about technological epistemology to be integrated into the philosophical and technical corpus. Since the working assumption of epistemology is that knowledge is binary (true or false), and that justification is a matter of degree, the more technological knowledge a person has, i.e. "knowledge that is involved in the designing, making and using of technical artifacts and systems" (Meijers & De Vries 2009, p. 70), the more a person can justify and defend the acceptance of a belief that was formed through the technological artifact. This means that the successful application of an epistemological framework that analyzes technology must take technological knowledge into its considerations. Nevertheless, technological knowledge was intellectually-historically neglected (Laudan 1984), and as Meijers & De Vries (2009, p. 70) note, "reflections on the nature of technological knowledge are fairly recent in the philosophy of technology. In more general epistemological debates, technological knowledge hardly ever features as an object of serious considerations". This paper constitutes an initial step in remedying this situation.

A Departure from Common and Accepted Views of Knowledge: the Example of Network Epistemology and the Generation and Distribution of Knowledge

After the IoT has been introduced and it was argued that knowledge in technological contexts hardly ever features epistemological analysis, this section suggests a reason for the lack of epistemic involvement in the

[2]For technical details see Hassan, Song, & Huh (2009) and Yuriyama & Kushida (2010).

[3]Jaffe, Mark. 2014. "IoT Won't Work Without Artificial Intelligence", Wired November 12, 2014. http://www.wired.com/2014/11/iot-wont-work-without-artificial-intelligence/

[4]Greenough, John. 2014. "The 'Internet of Things' Will Be The World's Most Massive Device Market and Save Companies Billions of Dollars", Business Insider November 5, 2014. http://www.businessinsider.com/how-the-internet-of-things-market-will-grow-2014-10

[5]Nevertheless, there are epistemologists who analyze technology and depart from common traditional views. This point will be further discussed in §2.2.

analysis of technology. It also attempts to remedy this situation with an initial epistemic comparison between human networks and networks of devices, and the analysis of IoT and Trust. Traditional views of epistemology are argued to lack the ability of analyzing current and future networked technologies, such as the IoT and SIoT. In contrast, a new kind of epistemological approach, *Techno-Epistemology*, is presented as a means to epistemically analyze technologies. It is argued that knowledge is not only a social phenomenon, but also a technological one. This section concludes with pointing out some epistemic differences between a group of humans and a group of networked devices, such as the IoT or SIoT, in order to lay the groundwork for the next sections to discuss the concept of trust, in a technological sense, and reveal the ethical considerations we must take in respect to trust in the IoT. Let us begin by briefly presenting the historical development of individual and social epistemology, and one of its criticisms, namely anthropocentric bias.

The Quests of Individual and Social Epistemology

Defined widely, epistemology is the study of knowledge. Though various kinds of knowledge exist, such as knowing a place, a person, or how to do something (like swimming), the scholarly interests of Anglo-American analytic epistemologists traditionally focus more narrowly - on the knowledge of propositions. (Steup 2014) That is, if people know what they believe, they would easily agree that a subject *S* knows a proposition *P* only if *S* believes that *P*. However, since Greek antiquity, a belief is not considered to be a sufficient condition. Since then, it was generally agreed that a subject *S* knows a proposition *P* only if *S* believes *P*, and in addition - that *P* is true. Similar to Socrates's arguments in *Meno* and in the *Theatetus*, if a person, out of the blue, superstitiously, or luckily guesses something that happens to be true, we would not consider the true belief as knowledge. The true belief must be tied to something else – a justification. Epistemologists referred to justification as that missing "something else", and as part of the three conditions for knowledge – justified, true belief [JTB].

After centuries of absence from intellectual discourse, the problem of what that "something else" is - has re-emerged. The JTB account of knowledge was refuted by Edmund Gettier's (1963) influential (among epistemologists) paper which introduced counter-examples to the (then) widely-accepted view. Gettier's argument, that one can have a JTB that is not knowledge, sparked the interest of epistemologists. Ever since, many new theories of knowledge were, and still are, being proposed, and have attempted to add more conditions or change the notion of justification.[6]

It was only relatively recently that philosophers began to engage with social epistemology[7]. Social epistemology deals with the social dimensions of knowledge. Generally, the term "knowledge", in its social sense, refers to epistemic content that has passed social processes, but the meanings of "social" and "knowledge" are both debatable. Scholars of social epistemology can be placed on a spectrum: those whose work is in keeping with the tenets of traditional individual epistemology, and those who depart from it. The first are referred to as *classical social epistemologists* or as the *orthodox camp*. They focus on concepts such as truth and rationality, and the ways in which an individual acquires knowledge or justified belief in social contexts. They build upon individual (general) epistemology and extend its scope to the social. The latter, *anti-classical social epistemologists*, or *reformists*, hold that knowledge, similar to language, is found within a community. They focus on collective doxastic agents or groups as another ontological level of knowledge bearing. The more extreme trends on this side of the spectrum, the *revisionist camp*, even reject the traditional focus on concepts such as justification or rationality. They "posit the social, practical, and empirical fruits of inquiry, rather than truth, as the standards of normative epistemic appraisal" (Miller forthcoming).

[6] This phenomenon has received an epithet label within scholar discussions, academic syllabuses, and publications – Gettierology. See Shope (1983) for the intellectual history of this quest.

[7] For the development of social epistemology, see Goldman & Blanchard (2012) and Miller (forthcoming).

Departing From Traditional Epistemology

Dealing with a wide variety of sources and processors of knowledge and justifications, such as sophisticated scientific instruments or computer software, significantly affects "our notion of science and scientific interpretation of the world, driving at the same time the philosophical debate[s]" (Primiero 2014, abstract). To a large extent, part of our knowledge, like many of our beliefs, is acquired, transmitted, generated, and mediated in and through technologies. Various scholars, theories, and approaches, outside of traditional epistemology attribute morality or the ability to know to technological artifacts. These views can be found within the fields of machine ethics (Torrance 2009), artificial intelligence (Tonkens 2009), and information ethics (e.g. Capurro 2000; Capurro & Hjørland 2003; Wallach & Allen 2009; Floridi & Sanders 2004). These views are also held by a number of scholars in Science and Technology Studies (e.g. Winner 1985; Latour 1992), phenomenologist philosophy, as well as some scholars who deal with information communication technologies. While attributing technology with the ability to know may be trivial to many scholars, traditional Anglo-American analytic epistemology, whether individual or social, does not attribute knowledge to artifacts. Individual epistemology concepts such as belief, proposition, memory, and causal reasoning, as well as social epistemology concepts such as testimony, evidence, and trust, are anthropocentric.

To a lesser degree, the ability to outsource knowledge (and understanding) to digital devices (e.g. via algorithms) is the defining feature of some philosophical approaches to technology (such as phenomenological digital ontology, see Eldred 2011; Compton 2009). It can be said that an analog to this outsourcing is found within the field of epistemology: some *reformist social epistemologists* do accept that mental states and cognitive processes extend beyond our organisms to other humans and artifacts[8]**.** As some scholars utilize traditional concepts, in general, to analyze knowledge *from* technology (e.g. Kourken 2014; Record 2013), this kind of analysis is not commonly found and is mostly believed to be limited. For example, David Coady, whose focus is applied epistemology, wrote in the preface to his (2012) book *What to Believe Now*:

> The information revolution and the knowledge economy have radically changed the way that we acquire knowledge and justify our beliefs. These changes have altered our epistemic landscape as surely as the sexual revolution and breakthroughs in reproductive technology have changed our moral landscape. The latter changes provided a good deal of the impetus for the applied turn in ethics, but the former *changes have so far failed to result in a comparable turn in epistemology. Such a turn is surely inevitable*. (p. 2, emphasis added)

Given the wide range of approaches to the relationship between technology and knowledge, how can epistemologists consider the place of technologies in various epistemic processes? Humphreys (2009) criticizes individual and social epistemological frameworks for being "infused with anthropocentric concepts" (p. 221). His criticism, based on the view that epistemology might be outdated, argues that today's technologies are looked to and used as sources of knowledge, as if they possess it: "[...] we do speak of computers storing and processing knowledge as well as information, language that is not just metaphorical. Printed books contain knowledge and so do their on-line versions" (ibid).

Revisionist social epistemologists seek to revise traditional epistemic notions for the epistemic analysis of knowledge and technology. For example, Baird (2004) developed material epistemology, and argued that (some) scientific instruments are a form of material objective knowledge and referred to them as "thing knowledge". Among the properties of thing knowledge is that it expresses the knowledge of their designers. Therefore, among other implications, technological knowledge is not belief-based, but thing-based[9] (for epistemic concerns, see Pitt 2007 and Kletzl 2014; for social concerns, see Cavicchi 2005). Other suggestions

[8] This is the internalism-externalism debate within epistemology regarding belief justifications that is parallel to the philosophy of mind internalism-externalism debate regarding the spatial location of cognitive processes and mental states (see Carter, Kallestrup, Palermos & Pritchard 2014). Externalists mostly rely on the extended cognition hypothesis (Clark 2007), the extended mind thesis (Clark & Chalmers 1998), and the distributed cognition hypothesis (Hutchins 1995).

[9] Within the phenomenological tradition, Eldred (2011, pp 61-62) recognizes know-how as a kind of understanding which is deeper than knowledge. He used a potato peeler as an example for outsourcing know-how knowledge (of peeling potatoes) to material design: "A

include different Truth criteria, such as effectiveness or efficiency, have also been raised (e.g. Houkes 2006). Nevertheless, technological knowledge (see §1.) is described as "epistemologically unusual" (Ibid). This makes the analysis of knowledge *from* technology much more complex (see §3.3.)

Techno-Epistemology in Brief

Whether or not epistemological approaches are correct in adhering to an anthropocentric approach to technology, they are nevertheless capable of applying their (limited) analyses on issues of technology. As mentioned before (§2.2.), these kinds of analyses are not commonly found. As Miller & Record (2013, p. 121) point out: "despite our vast and deep dependence on technology for acquiring knowledge and justified belief, epistemology has not, for the most part, given serious thought to the role technology plays in the fabric of knowledge and justification".

Some areas of science such as robotic astronomy, parts of experimental high energy physics, and parts of genomic analysis, can be said to present instruments that collect data that is processed by computers without any intervention by humans (Humphreys 2009). The trend of purely automated processes, carried out by scientific networks of instruments and computers, is increasing. The same thing could be said about the IoT and its usage within the scientific domain. Scientists and scholars will not only develop and discuss the IoT, but will also use it for their own research – as scientific instruments that create and measure phenomena. Let us refer to the IoT devices that can be applied to a scientific use, such as the aforementioned purely automated processes, as *Scientific Instruments of Things* [SIoT]. In order to epistemologically address the IoT, SIoT, and technologies in general, we need to carefully depart from the traditional individual and social epistemological layers of analysis, and without rejecting them form a new one – technological. Let us refer to this layer as *Techno-Epistemology* (see table 1).

Table 1. A Proposal for a New Epistemic Approach

Layers of epistemic analysis	*Techno-Epistemology*		
	Social Epistemology		
	Individual Epistemology		
Unit of analysis	Individual	Social	Technological

Techno-Epistemology's layer of analysis can take into consideration the individual, social, and technological units of analysis.

Knowledge Generation and Distribution: Epistemic Differences Between Social and Technological Analysis

Miller & Pinto (in progress) note three major, fundamental and widely-accepted views of the generation and distribution of scientific knowledge: Kitcher's (1990) description of apt division of cognitive labor among researchers, Longino's (2002) description of the social process of critical scrutiny and evaluation, such as peer review, that information must undergo in order to acquire the status of knowledge, and Hardwig's (1985) cornerstone paper about justified relations of trust among researchers.

This paper offers an in-principle epistemic symmetry between human and non-human epistemic agents regarding the generation and distribution of scientific knowledge. Since the generation and distribution of knowledge, in general, are not only social processes, but also technological processes, we are behooved to extend, or even revise, our epistemic views. A hybrid view of knowledge generation and distribution, for both human and non-human epistemic agents, as well as both the social and the technological processes involved, is needed in order to properly epistemically analyze technologies in general, and the IoT in particular. The future trend of SIoT

better potato peeler is the embodiment of a better, more efficient potato-peeling know-how" (p. 62). Within the analytic tradition, other examples for revisionist social epistemologists are, for example, Chang (2004) and Humphreys (2004).

exemplifies technologies which take part in the generation and distribution of scientific knowledge. *Techno-Epistemological* analysis that takes into account the major epistemic differences between networks of humans and machines, as Humphreys (2009) initially suggested, in the context of the networked devices of the IoT and the SIoT is proposed.

While no single scientist can directly access the knowledge of another peer, SIoTs may have direct access to networked knowledge. Also, the network of SIoT can perform a kind of a "thought transfer", to a degree that a device inside the network can reason or conclude from the data, information, or knowledge that is transferred, generated, or directly accessed through the network. Another major epistemic difference is the kind of subjectivity that is common among scientists' beliefs and background beliefs regarding scientific knowledge: while a humanitarian belief regarding science cannot always be explicitly expressed and communicated (and if so, it is sometimes considered subjective), the propositions of machines or models that take part in the SIoT *can* be explicitly expressed.

Finally, the network of the SIoT can, in principle, epistemically act as a single agent, while a community of scientists exchanging knowledge will not act as immediately and as directly as the networked SIoT. Given the differences between human networks and networks of IoT and SIoT, how can human users trust the networked devices of the IoT, and how can justified relations of trust form between scientists the SIoT?

Trust as a Cornerstone Characteristic in the Construction of the IoT

In the previous sections, this paper argued that individual and social epistemologies are anthropocentrically biased, and therefore insufficient for analyzing networked technologies. The framework of *Techno-Epistemology* was proposed as a third epistemic approach that can be used to analyze networked technologies such as the IoT and SIoT. The next section points out the ethical considerations of *Techno-Epistemology* through the prism of the topic of trust. It begins by presenting the commonly-found distinction between trust and reliance, and the various approaches that different fields of inquiry take toward it. I show that epistemology considers the possession of human qualities that enable morality to be a fundamental requirement for an epistemic agent to trust or to be trusted. Other accounts of agents that require human qualities to lesser extents are presented. By building on those other accounts, this paper presents the concepts of trust regarding epistemic agents in a way that avoids the anthropocentric bias of traditional epistemic requirements. This results in a different epistemological perspective that opens up for analysis conceptions of trust outside of the traditional relationships formed exclusively between human beings. In light of this perspective, the epistemic, social, and ethical layers of trust are discussed. Section 4 will present *Techno-Trust* in the context of the layers of trust discussed in Section 3, and Section 5 will conclude by presenting the formation of a trustworthy LSSTS.

The Trust-Reliance Distinction and Non-Moral Epistemic Agents

In recent years, the concept of *trust* has been widely discussed in many academic contexts and disciplines, mostly in computer science, management, and business[10]. Different applications and understandings of trust have developed across the many fields in which it is discussed. In epistemology, the topic of trust is mostly discussed within the context of testimonial accounts of knowledge[11], though "there are a number of philosophical questions that arise in relation to the concept of trust, both because of the intrinsic interest of the topic, and also because it is so fertile a perspective from which to approach different topics related to the way we live together" (Simpson 2012, p. 566).[12]

[10] As indicated by Thomson Reuters' Web of Science. Search criteria: Topic: "Trust", Timespan: All years, Indexes: SCI-EXPANDED, SSCI, A&HCI, CPCI-S, CPCI-SSH.

[11] Though the concept of testimony is not elaborated in this paper, it is shortly discussed in §4 and footnotes 16 and 18.

[12] Simpson (2012) notes that "the philosophical literature on trust remains slim indeed" (p. 550), that "there is no single phenomenon that 'trust' refers to" (p. 551), and makes the case that the concept of trust is not amenable to conceptual analysis as it is as an umbrella

The spectrum of the extent to which a notion of trust can be applied to non-humans – such as technological artifacts, scientific instruments, or even LSSTS's – ranges according to the discipline's accepted views. As mentioned before (§2.2.), at one extreme, scholars within the field of Science and Technology Studies [STS] argue that technological artifacts possess a form of agency of their own (canonical examples are Winner 1985 and Latour 1992[13]). In the corpora of a few disciplines, such as information ethics (e.g. Wallach & Allen 2009; Floridi & Sanders 2004), machine ethics (Tonkens 2009), and artificial intelligence (Torrance 2011), it is acceptable and common for a non-human epistemic agent to act as a moral agent, and therefore to be able to trust or be trusted (e.g. Tavani 2014).

At the other extreme, some philosophers of technology, famously influenced by Joseph Pitt's "technology is *humanity* at work" (2010, p. 445, originally emphasized; see 1983 for the original formulation) tend to take an opposite viewpoint, and reduce questions regarding trust in technologies to questions regarding trust in the humans which are "behind" these technologies, such as designers or engineers. Within normative ethics and epistemology discourses, the general and accepted view is that a human cannot form trust relationships with a non-moral agent. Trust, many hold, is founded on a human quality, such as rationality, consciousness, free will, intentionality, and so forth. For example, Jones (1996, p. 14) stated that "trusting is not an attitude that we can adopt toward machinery […] One can only trust things that have wills, since only things with wills can have goodwills". The latter camp argues that though we cannot trust technological artifacts, we can rely on them: "reliance is way of acting, whereas trust is an attitude" (Nickel 2013, p. 224 fn 3). Trustworthiness, unlike reliability, is "the opportunity for the trustee to act against the wishes of the trustor and the trustee's consideration of the value of the trust that has been placed in them by the trustor" (Wright 2010, abstract).

The trust-reliance distinction, in its technological context, focuses on the question of whether or not trust relationships, involving both humans (as moral agents) and non-humans (as non-moral agents), are possible. Human qualities required for such a relationship, such as those stated above, are not (yet) possessed by technological artifacts, which cannot be considered as moral agents – and therefore cannot be considered trustable.

The late Edsger Dijkstra, a computer scientist, once said that "the question of whether machines can think [...] is about as relevant as the question of whether submarines can swim"[14]. The same could be said about many human activities. The case of trust exemplifies the limits of epistemology in its considerations of non-humans. More generally, "it seems that the difficulties [...] lie in the tendency of standard epistemology to analyze knowledge in terms of human beings' properties" (Miller & Record, p. 121).

However, it is possible to build upon conceptual epistemological advances that have been made regarding technological artifacts**.** For example, Johnson (2006) does not consider technological artifacts to be moral agents, but argues that they do have "moral efficiency" and therefore qualify as "moral entities". Floridi (2011) argues that autonomous technological artifacts (what he terms *Autonomous Artificial Agent*) can be moral agents since they can function as "sources of moral action" and are able to cause moral good or harm (Tavani 2014). The corpus that has dealt with the question of whether a technological artifact can be considered a moral agent is large enough to advance non-traditional views of moral technological agents. For example, Johansson (2013) lists various views about the possibility of an action that can "originate inside an artifact, considering that it is, at least today, programmed by a human" (p. 295).

Whether or not *Techno-Epistemology,* as a new epistemic layer of analysis, departs from the anthropocentric conceptions prevalent in individual and social epistemology and treats technological artifacts as epistemic agents, it can still analyze the role technology takes in knowledge and justification made by human(s). If it

term. I embrace this view; the various contents of the concepts of trust presented here are not necessary and sufficient conditions for a definition.

[13] Though other STSers such as Bloor (1999) and Collins (2010) have argued that humans differ from non-humans in the context of justification.

[14] Dijkstra, Edsger W. 1984. "The threats to computing science", Lecture delivered at the ACM 1984 South Central Regional Conference, November 16-18, Austin, Texas, USA. Transcript available at http://www.cs.utexas.edu/users/EWD/transcriptions/EWD08xx/EWD898.html

does depart from prevalent anthropocentric conceptions, it is inherent that the non-human epistemic agents (devices, instruments, algorithms, etc.), which can be regarded as outsourced human knowledge, can *normatively expect* that information from other sources be transmitted in a certain standardized form.[15] Without rejecting individual and social epistemology, *Techno-Epistemology* holds that relations of *techno-trust* can be formed between two non-moral agents, and between non-moral and moral agents. It is possible only if an epistemic agent, human or not, expects information to be provided in certain forms, and its attitude is affected by the information received. This point will be further elaborated in light of social epistemology's concept of testimony in Section 4.

By presenting the *trust-reliance* distinction, the concept of trust was presented as polysemous among various disciplines. By avoiding the anthropocentric bias of traditional requirements for morality or human qualities, it is possible to discuss trust not only as a relationship between two human beings, but also between humans and devices, as well as between devices. The next section begins with a distinction between epistemic and social trust, and present ethical trust as a link between these two.

Trust Between Humans and the Networked IoT

McDowell (2002) distinguishes between *epistemic trust* and *social trust,* and argues that they are deeply related. While epistemic trust regards justification of beliefs in propositions made by an epistemic agent, social trust "[…] is trust that someone will act co-operatively, or with one's best interests in mind, and in accordance with the social mores of the society or situation in which the participants find themselves" (p. 54). For example: I *epistemically trust* Adam, a know-it-all character - his statements are (probably) true. I do not *socially trust* Adam that he will keep it to himself if I ask him about Michelle. I *socially trust* my library not to share my loan history list with advertisers from the local book industry. Social trust can raise the amount of information interaction, as it "involves moral, personal or cultural dependability, or some combination of these" (p. 54).

Part of the upcoming challenge is not only to construct the IoT devices to be epistemically trustworthy by indicating that its truth statements are right (i.e. epistemic trust), but also to construct the system, as a whole, as trustworthy (i.e. social trust). This challenge would likely involve a wide variety of characteristics to consider. Such a characteristic might be, for example, transparency regarding the relevant information and processes disclosed: "in order to critically assess epistemic agents, content and processes, we need to be able to access and address them" (Simon 2010, p. 343).

The Formation of Epistemic Trust Between Humans and the IoT

Lehrer (1995) offers the *Evaluation Model of Instrumental Knowledge* for explaining the structure of justification for trustworthiness. Among the essential features of instrumental knowledge, is the acceptance of the trustworthiness of the instrument and its output as truth. In order to know *p* through the use of an instrument, a person must have a trustworthy basis for the evaluation of the belief and defend its acceptance against objections. But what is that trustworthy basis for the evaluation of the belief? Sosa (2006) presents an account of how not only our senses are reliable, but instruments as well[16]: a non-human technological artifact is reliable when a human subject has an indication that the artifact indicates the truth outright and accepts that indication.

It is possible, then, to consider what a framework for the formation of epistemic trust in the IoT and SIoT might look like. In order for a human subject (or a scientist) *S* to form epistemic trust in the IoT's (or in the SIoT's)

[15] For additional approaches which take this direction, see Buechner & Tavani (2011).

[16] Sosa (2006) argues that testimonial knowledge presupposes instrumental knowledge by using the instrument of language. Consequently, instrumental knowledge, including testimonial knowledge, cannot be reduced to non-instrumental knowledge: "Our access to the minds of others is after all mediated by various instruments, and we must trust such media at least implicitly in accessing the testimony all around us" (p. 118, originally emphasized). For the contrary view, see Goldberg (2012). See also §4 and footnote 18 for more on testimony in technological context.

devices' output, *S* must have an indication that the device indicates the truth, and accepts that indication. In addition, *S* must be able to defend the acceptance of the belief against objections. This means that knowledge regarding how the device resulted with its outcome, meaning technological knowledge, is needed.

The Ethical Dimension of Trust

The formation of trust is, in itself, ethical, but what is the ethical dimension of trust and what is its relation to epistemic and social trust? The ethical dimension of trust can serve as a link between epistemic and social trust. Wagenknecht (2014) argues that the moral dimension of trust does not involve doubts concerning the *epistemic trustworthiness* of a collaborator, i.e. the risk of doubts concerning the true or false value of a proposition. Instead, it involves "the deliberate will to take this risk and to resort to a number of measures that can mitigate it" (p. 85). By referring to "institutional trust, i.e. trust in community-borne gate-keeping functions, [the truster] can partly compensate for a lack of familiarity with potential collaborators" (ibid).

This lack of familiarity, which happens when a truster needs to co-operate with an unknown epistemic agent, forces trusters to rely on social norms and standards. Since trust is usually not something measured, but is rather an attitude expressed by one epistemic agent towards another, that attitude is mostly invisible. As Marsh & Briggs (2009, p. 10) stated: "like light, trust is seen in its effect on something, and in between truster and trustee, there is simply nothing to see".

Kiran & Verbeek (2010) argued that it is possible to actively engage in the technological processes that impact us. Trust, according to their argument, takes on the character of confidence: we trust ourselves *to* technology. This means our concern should be "how to take responsibility for the quality of technological mediations, and of our ways of living with these mediations" (p. 425). The ethical dimension of trust, which can be identified as the "unseen link" between epistemic trustworthiness and the social norms and standards which lets trusters take the risk of doubt, is where the challenge of social trust is focused: how can these social norms and standards be institutionalized, and how can they be embedded within the network of the IoT? Norms and standards are, after all, not only social but technological as well. The goal of making these norms and standards explicit, and the question of what are these norms and standards are, are left open for future experts, specialists, and users, to achieve and answer. With these answers it is possible to gain social, technological, and LSSTS kinds of trust.

The Formation of Social Trust Between Humans and the IoT

Kounelis *et al*. (2014) discuss the topic of trust in the context with the IoT. Their focus is not epistemological, but social and technical, mostly oriented toward democracy and security. By using the concept of "citizen", and not "user", they highlight that "the human capacity to maintain autonomy and control in a world of pervasive human-technological networking should be considered as an essential part of our ethical and legal endowment and entitlement in IoT" (p. 74). They suggest that by using a framework named *SecKit* (Security Kit), it is possible for citizens to adopt a collaborative approach to address various issues that regard the IoT, such as privacy or data protection (p. 77). Collaborations between humans, in order to pinpoint which technical and technological issues are important, increase the amount of information interaction, and form social trust between human users (or citizens, in Kounelis *et al*.'s case) and the IoT.

Nickel *et al.* (2010) recognize that any applicable notion of trustworthiness to technology must depart significantly from the notion of trustworthiness associated with interpersonal trust[17]. Nickel's (2013) account of trust involves trusting not only in the humans behind the technologies, but also in institutions. Though not all kinds of trust in technologies can be reduced to the humans and institutions behind them, he offers the *Entitlement Account* that makes sense of trust in technological artifacts. Two kinds of evidence will assure this kind of trust,

[17] See also Lahno (2004) for three accounts of interpersonal trust.

by indicating that the designers have strong interests in serving the interests of the users: 1) A failure to perform will lead to an effective sanction by institutional structures, and 2) others are willing to stake their reputations on the technologies' performances. Both approaches exemplify how social processes can alter the technological norms and standards. In order to form relations of trust with technological artifacts and with the IoT in particular, we must pay constant attention not only to the social, but also the technological norms and standards which regard trust.

Techno-Trust by a Reputation Cloud

In the preceding sections, the formation of epistemic trust between humans and instruments, as well as the formation of social trust, were discussed. The ethical layer of trust was identified as the "unseen link" between the two. This section extends the ethical layer of trust by offering an epistemic account of trust between machines, referred to here as *Techno-Trust*. To exemplify *Techno-Trust,* I suggest a reputation system upon which IoT and SIoT can form evidence-based trust relations.

Goldberg (2012) rejected the possibility that a non-human can reliably receive testimony from instruments. According to his view, to "rely in belief-formation on another speaker is to rely on an epistemic subject, that is, on a system which itself is *susceptible to epistemic assessment in its own right*, whereas 'mere' instruments and mechanisms are not properly regarded as epistemic subjects in their own right, they are *not susceptible to normative epistemic assessment*" (p. 182, emphasis added). Goldberg distinguished between *instrument-based beliefs* and *testimony-based beliefs.* The latter belong to epistemic subjects in their own right, "susceptible to full-blooded normative assessment" (p. 191), and "sophisticated enough to satisfy the conditions on being appropriately assessed in terms of rationality and responsibility" (p. 194). Without rejecting this view, the epistemic approach of *Techno-Epistemology* in principle deals with testimonies received by non-human epistemic agents that are not "full-blooded"[18].

Sometimes "a person is not trusting another person but is instead trusting the community to which they both belong to tell them whether or not trust can be given [...] If someone does not live up to the community expected standards, then [the trustee] receives bad reviews, lowering their reputation" (Lawrance 2009, p. 327). According to this view, whenever expectations are not met, the reputation of the trustee is lowered, and potential trusters would gradually cease to trust the poorly reviewed epistemic agent.

By adopting this reasoning, the suggestion is to form a reputation system for devices, which serves as a provider of explicit qualitative and objective measurements of the trustworthiness, as reflected by the characteristics of the device in question. This reputation system can be seen as a basis for the formation of *techno-trust* relations between devices of the IoT. Moreover, if evidence for trustworthiness is available to a human truster, a rational basis for trust can be formed (Simpson 2011; for the analysis of reputation as phenomenological phenomena, see Eldred 2013).

Since most interaction within the network of the IoT and SIoT is machine-to-machine interaction, the basic idea is to form a system that will assist devices in choosing their sources: the devices rate the interactions with each other on the basis of their observed and measured behavior, and base their interactions on these ratings.[19] In this way, each device "consults" the reputation cloud for the necessary information that is crucial for its own decision making, beyond an evaluation of how well they perform the tasks they were designed for. For example, for one type of device, the normative expectation to get a result immediately might be the main characteristic of trust, while for another, the frequency of sensors calibration, or the kind of lens it has, might be the crucial factors for the automated decision making process. Through this method a device will improve (or worsen) its

[18] Miller & Record (2013, p. 121, fn 3) correctly stated that "the question of whether and on what conditions information from computers and other instruments constitutes testimony has been largely overlooked". For exceptions, see references within and footnote 16 of this paper.

[19] For a survey of multi-agent trust models, see, e.g., Han et al. (2013); and for a survey of surveys, see Pinyol & Sabater-Mir (2013).

reputation for various functions, and thus acquire (or revoke) its ability to be *techno-trusted* by other IoT devices.[20]

Conclusion: The Formation of Trustworthiness in Large-Scale Socio-Technological Systems

Let us briefly recall the various accounts of rely and trust. Epistemic trust is assured by Sosa's (2006) *Basis for the Evaluation of the Belief* which holds that a technological artifact is reliable when a human subject has an indication that the artifact indicates the truth outright and accepts that indication. Building on the trustworthy basis for the evaluation of the belief, Lehrer's (1995) *Evaluation Model of Instrumental Knowledge* demands an ability to defend the acceptance of the belief against objections.

Social trust is exemplified by Kounelis *et al.*'s (2014) suggestion for citizens (human users) to maintain their autonomy and control by adopting a collaborative approach to address various social issues relating to the IoT. Social trust can also be ensured by Nickel's (2013) suggestion for evidence that humans behind the technologies, such as designers and manufacturers, have strong interest in serving the interests of the users. This can be indicated by effective sanctions levied by institutional structures, in the case of a failure, and by the fact that others are willing to stake their own reputation by using the technology. Both approaches exemplify how social norms and standards affect technological norms and standards.

The IoT devices rate the interactions with each other on the basis of their observed and measured behavior, and base their interactions on these ratings. This kind of reputation system presents evidence for trustworthiness, forming *techno-trust* between devices, and serves as a basis for the rational formation of trust in these devices by humans. The reputation system can be seen as the embedment of standards in the network of the IoT. The trustworthiness of a LSSTS, then, is assured by all layers of trust.

The main arguments were that an adequate theoretical, systematic epistemic framework that analyzes technology must be developed, and that the ethical layer of trust is what ties the other layers discussed in this paper. Ethical trust, or the deliberate will to take epistemic risks by referring to social trust, to use McDowell's (2002) distinction, is the dimension of trust which lets trusters take the risk of doubt by leaning on social norms and standards (Wagenknecht 2014). These social norms and standards affect technological norms and standards. It was claimed that trust is "unseen" (Marsh & Briggs 2009) and that we have the responsibility to actively engage in technological processes (Kiran & Verbeek 2010). Therefore, "unseen" desired norms and standards regarding trust, both social and technological, must be revealed, explicitly expressed, institutionalized, and embedded in the network of the IoT. They should be implemented in our collaborative use of technologies, the activities of institutions, and the design of technological artifacts. These norms and standards set the level of epistemic, social, technological, and LSSTS trust. The ethical dimension of trust constitutes a link between epistemic trust and other layers of trust. It constitutes our responsibility to reveal desired trust-related social and technological norms and standards and embed them in other frameworks of trust.

20See Marsh & Briggs (2009) for formalizations, as computational concepts, of regret and forgiveness in the context of trust. For more on reputation in the context of the cyberworld, see special issue of International Review of Information Ethics, vol 19.

Table 2. Frameworks of Trust

Layers of trust	Large-Scale Socio-Technological System			
	Epistemic	Ethical	Social	Technological
Particular accounts suggested	Sosa (2006), Lehrer (1995)	Marsh & Briggs (2009), Wagenknecht (2014), Kiran & Verbeek (2010)	Kounelis *et al*. (2014), Nickel (2013)	Simpson (2011), Lawrance (2009)
Focus of trust	Instruments	"Unseen" norms and standards made explicit, responsibility	Collaborative approach, institutions' regulations	Reputation cloud

The ethical layer of trust is bolded as this layer constitutes the link between epistemic trust and the other layers of trust. All accounts of trust form a trustworthy LSSTS.

References

Baird, Davis. 2004. Thing Knowledge: A Philosophy of Scientific Instruments. University of California Press.

Bloor, David. 1999. "Anti-Latour", Studies in History and Philosophy of Science 30(1): 81-112.

Buechner, Jeff & Tavani, Herman T. 2011. "Trust and multi-agent systems: applying the 'diffuse, default model' of trust to experiments involving artificial agents", Ethics and Information Technology, 13(1): 39-51.

Capurro, Rafael & Hjørland, Birger. 2003. "The Concept of Information", Annual Review of Information Science and Technology 37(1): 343-411.

Capurro, Rafael. 2000. "Hermeneutics and the phenomenon of information", In Metaphysics, Epistemology, and Technology. Research in Philosophy and Technology. Vol. 19, Carl Mitcham (ed.), JAI/Elsevier Inc. 2000, pp. 79-85.

Carter, A. J., Kallestrup, J., Palermos, O. S., & Pritchard, D. 2014. "Varieties of Externalism", Philosophical Issues 24: 64-109.

Cavicchi, Elizabeth. 2005. "Thing Knowledge: A Philosophy of Scientific Instruments (review)", Technology and Culture 46(1): 243-245.

Chang, Hasok. 2004. Inventing Temperature. Measurement and Scientific Progress. Oxford: Oxford University Press.

Clark, Andy & Chalmers, David. 1998. "The Extended Mind", Analysis 58: 7-19.

Clark, Andy. 2007. "Curing Cognitive Hiccups: A Defense of the Extended Mind", Journal of Philosophy 104: 163-192.

Coady, David. 2012. What to Believe Now: Applying Epistemology to Contemporary Issues. Wiley-Blackwell.

Collins, Harry M. 2010. "Humans not Instruments", Spontaneous Generations: A Journal for the History and Philosophy of Science 4(1): 138-147.

Compton, Bradley Wendell. 2009. The Domain Shared by Computational and Digital Ontology: a Phenomenological Exploration and Analysis. Electronic Theses, Treatises and Dissertations. Paper 3484, Florida State University.

Eldred, Michael. 2013. "Reputation in the Cyberworld", International Review of Information Ethics 19: 4-11.

Eldred, Michael. 2011 [2009]. The Digital Cast of Being: Metaphysics, Mathematics, Cartesiansim, Cybernetics, Capitalism, Communication. Gazelle Books Services. http://Arte-fact.org/dgtlcast.pdf

[ERCIT] European Research Cluster on the Internet of Things. 2012. The Internet of Things 2012 - New Horizons. Smith, Ian G. (ed.) Halifax, UK: New Horizons.

Floridi, Luciano & Sanders Jeff W. 2004. "On the Morality of Artificial Agents", Minds and Machines 14(3): 349-379.

Floridi, Luciano. 2011. "On the Morality of Artificial Agents", In Machine ethics, M. Anderson and S. L. Anderson (Eds.), Cambridge University Press, pp. 184-212.

Gettier, Edmund. 1963. "Is Justified True Belief Knowledge?", Analysis 23(6): 121-123.

Goldberg, Sanford C. 2012. "Epistemic extendedness, testimony, and the epistemology of instrument-based belief", Philosophical Explorations: An International Journal for the Philosophy of Mind and Action 15(2): 181-197.

Goldman, Alvin I & Blanchard, Thomas. 2012. "Social Epistemology", In Oxford Bibliographies Online.

Han, Yu, Zhiqi, Shen, Leung, C., Chunyan Miao, & Lesser, V.R. 2013. "A Survey of Multi-Agent Trust Management Systems", Access, IEEE 1(1): 35-50.

Hardwig, John. 1985. "Epistemic Dependence", The Journal of Philosophy 82(7): 335-349.

Hassan, M. M., Song, B., & Huh, E. 2009. "A framework of sensor-cloud integration opportunities and challenges", In Proceedings of the 3rd International Conference on Ubiquitous Information Management and Communication, ICUIMC 2009, Suwon, Korea, January 15–16, pp. 618–626.

Houkes, Wybo. 2006. "Knowledge of Artefact Functions", Studies in History and Philosophy of Science 37: 102-113.

Humphreys, Paul. 2004. Extending Ourselves: Computational Science, Empiricism, and Scientific Method. Oxford: Oxford University Press.

Humphreys, Paul. 2009. "Network Epistemology", Episteme 6(2): 221-229.

Hutchins, Edwin. 1995. Cognition in the Wild. Cambridge, MA: MIT Press.

Johansson, Linda. 2013. "The Pragmatic Robotic Agent", Techné: Research in Philosophy and Technology 17(3): 295-315.

Johnson, Deborah G. 2006. "Computer systems: moral entities but not moral agents", Ethics and Information Technology 8(4): 195-204.

Jones, Karen. 1996. "Trust as an Affective Attitude", Ethics 107(1): 4-25

Kiran, Asle H. & Verbeek, Peter-Paul. 2010. "Trusting Our Selves to Technology", Knowledge, Technology & Policy 23(3-4): 409-427.

Kitcher, Philip. 1990. "The Division of Cognitive Labor", The Journal of Philosophy 87(1): 5-22.

Kletzl, Sebastian. 2014. "Scrutinizing thing knowledge", Studies in History and Philosophy of Science Part A 47: 118-123.

Kounelis, I.,Baldini, G., Neisse, R., Steri, G., Tallacchini, M., and Guimaraes Pereira, A. 2014. "Building Trust in the Human? Internet of Things Relationship", Technology and Society Magazine, IEEE 33(4): 73-80.

Kourken, Michaelian. 2014. "JFGI: From Distributed Cognition to Distributed Reliablism", Philosophical Issues, A Supplement to NOUS 24: 314-346.

Lahno, Bernd. 2004. "Three Aspects of Interpersonal Trust", Analyse & Kritik 26: 30-47.

Latour, Bruno. 1992. "Where are the missing masses? The sociology of a few mundane artifacts", In Shaping Technology/Building Society; Studies in Sociotechnical Change, Bijker and Law (eds.). Cambridge: MIT Press, pp. 225-258.

Laudan, Rachel. 1984. The Nature of Technological Knowledge. Are Models of Scientific Change Relevant? Boston: Reidel.

Lawrance, Faith K. 2009. "Internet-Based Community Networks: Finding the Social in Social Networks", In Computing with Social Trust, Jennifer Golbeck (ed.), Springer, pp. 313-332.

Lehrer, Keith. 1995. "Knowledge and the Trustworthiness of Instruments", The Monist 78(2):156-170.

Longino, Helen. 2002. The Fate of Knowledge. Princeton: Princeton University Press.

Marsh, Stephen & Briggs, Pamela. 2009. "Examining Trust, Forgiveness and Regret as Computation Concepts", In Computing with Social Trust, Golbeck, Jennifer (ed.). Springer, pp. 9-43.

McDowell, Ashley. 2002. "Trust and information: The role of trust in the social epistemology of information science", Social Epistemology 16(1): 51-63.

Meijers, Anthonie W. M. & Marc J. De Vries. 2009. "Technological Knowledge", In A Companion to the Philosophy of Technology, Olsen, J.K.B., Pedersen, S.A. and Hendricks, V.F. (eds). Chichester: Wiley-Blackwell, pp. 70-74.

Miller, Boaz & Pinto, Meital. In progress. "Epistemic Equality".

Miller, Boaz & Record, Isaac. 2013. "Justified Belief in a Digital Age: On the Epistemic Implications of Secret Internet Technologies", Episteme 10(2): 117-134.

Miller, Boaz. Forthcoming. "Social Epistemology", In The Internet Encyclopedia of Philosophy.

Nickel, Philip. J. 2013. "Trust in Technological Systems", In Norms in Technology, M. J. de Vries et al. (eds.). Dordrecht: Springer, pp. 223-237.

Nickel, Philip J., Franssen, Maarten, & Kroes, Peter. 2010. "Can We Make Sense of the Notion of Trustworthy Technology?", Knowledge, Technology & Policy 23(3-4): 429-444.

Pinyol, Isaac & Sabater-Mir, Jordi. 2013. "Computational trust and reputation models for open multi-agent systems: a review", Artificial Intelligence Review 40: 1-25.

Pitt, Joseph C. 1983. "The epistemological engine", Philosophica 32(2): 77-95.

Pitt, Joseph C. 2007. "Speak to Me", Metascience 16: 51–59.

Pitt, Joseph C. 2010. "It's not about technology", Knowledge, Technology and Policy 23(3-4):445-454.

Primiero, Giuseppe. 2014. "On the Ontology of the Computing Process and the Epistemology of the Computed", Philosophy and Technology 27(3): 485-489.

Record, Isaac. 2013. "Technology and Epistemic Possibility", Journal for General Philosophy of Science 44: 319-339.

Shope, Robert K. 1983. The Analysis of Knowing: A Decade of Research. Princeton University Press.

Simon, Judith. 2010. "The Entanglement of Trust and Knowledge on the Web", Ethics and Information Technology 12:343-355.

Simpson, Thomas W. 2011. "E-Trust and Reputation", Ethics and Information Technology 13(1): 29-38.

Simpson, Thomas W. 2012. "What is Trust?", Pacific Philosophical Quarterly 93: 550–569.

Sosa, Ernest. 2006. "Knowledge: Instrumental and Testimonial", In The Epistemology of Testimony, J. Lackey and E. Sosa (eds.). Oxford: Oxford University Press, pp. 116-123.

Stankovic, J.A. 2014. "Research Directions for the Internet of Things", Internet of Things Journal, IEEE 1(1): 3-9.

Steup, Matthias. 2014 [2005]. "Epistemology", In The Stanford Encyclopedia of Philosophy, Edward N. Zalta (ed.). http://plato.stanford.edu/archives/spr2014/entries/epistemology

Tavani, Herman T. 2014. "Levels of Trust in the Context of Machine Ethics", Philosophy and Technology, Published Online 3 May 2014.

Tonkens, Ryan. 2009. "A Challenge for Machine Ethics", Minds And Machines: Journal For Artificial Intelligence, Philosophy, And Cognitive Science 19(3): 421-438.

Torrance, Steve. 2011. "Machine ethics and the idea of a more-than-human moral world", In Machine Ethics, M. Anderson and S. Anderson (Eds.). Cambridge Univ. Press, pp. 115-137.

van den Dam, Rob. 2013. "Internet of Things: The Foundational Infrastructure for a Smarter Planet", In Internet of Things, Smart Spaces, and Next Generation Networking, Lecture Notes in Computer Science Volume 8121, pp. 1-12.

Wagenknecht, Susann. 2014. "Four Asymmetries Between Moral and Epistemic Trustworthiness", Social Epistemology Review and Reply Collective 3(6): 82-86.

Wallach, Wendell & Allen, Colin. 2009. Moral Machines: Teaching Robots Right from Wrong. Oxford: Oxford University Press.

Winner, Langdon. 1985. "Do artifacts have politics?", In The social shaping of technology, Mackenzie and Wajcman (eds.). Milton Keynes: Open University Press.

Wright, Stephen. 2010."Trust and Trustworthiness", Philosophia 38: 615–627.

Yuriyama, M. & T. Kushida. 2010. "Sensor-Cloud Infrastructure – Physical Sensor Management with Virtualized Sensors on Cloud Computing", NBiS: 1-8.

Caroline Rizza and Laura Draetta:

The "silence of the chips" concept: towards an ethics(-by-design) for IoT

Abstract:

In this position paper, we would like to promote the alternative approach positioned between the two extreme positions consisting in refusing any innovation or in adopting technology without questioning it. This approach proposes a reflexive and responsible innovation (von Schomberg, 2013; 2011; 2007) based on a compromise between industrial and economic potentialities and a common respect of our human rights and values. We argue that the "silence of the chips right" (Benhamou, 2012; 2009) is timely, relevant and sustainable to face ethical challenges raised by IoT such as protecting privacy, trust, social justice, autonomy or human agency. We believe this technical solution may support establishing an ethics of IoT embedded in the technology itself. Our position is not 'technocratic': we do not agree with discourses arguing technology can fix problems. Through the responsible research and innovation approach we promote the idea that only human agency and user empowerment constitute a valid answer to the ethical, legal and social issues raised by IoT.

Agenda:

Authors:

Caroline Rizza, PhD,

- Associate Professor, Economics, Management and Social Sciences Department, Institut Mines Telecom / Telecom ParisTech, I3 UMR 9217 – CNRS. 46 Rue Barrault 75634 Paris Cedex 13 - France
- ☎ + 33 - 145 - 81 81 35, ✉ caroline.rizza@telecom-paristech.fr
- Relevant publications:
  - Curvelo P, Guimarães Pereira Â, Boucher P, Breitegger M, Ghezzi A, Rizza C, Tallacchini M, Vesnic-Alujevic L (2014). The constitution of the hybrid world: How ICTs are transforming our received notions of humanness. EUR, VARESE: Luxembourg: Publications Office of the European Union, doi: 10.2788/58678
  - Rizza C, & Guimarães Pereira A, Ed.(2013)."Ethics of Social Networks for Special Needs Users". ETHICS AND INFORMATION TECHNOLOGY, Springer: Netherlands.
  - Rizza C, Curvelo P, Crespo I, Chiaramello M, Ghezzi A, & Guimarães Pereira Â (2011). Interrogating privacy in the digital society: media narratives after 2 cases. INTERNATIONAL JOURNAL OF INFORMATION ETHICS, vol. 16, p. 6-17.

ISSN 1614-1687

Laura Draetta, PhD,

- Associate Professor, Economics, Management and Social Sciences Department, Institut Mines Telecom / Telecom ParisTech, I3 UMR 9217 – CNRS. Campus SophiaTech, 450 Route des Chappes - 06410 Sophia Antipolis – France.
- ☎ + 33 - 493 - 00 84 09, ✉ laura.draetta@telecom-paristech.fr http://email/
- Relevant publications:
  - Draetta L. et Delanoë A., 2012, RFID une technologie controversée. Ethnographie de la construction sociale du risque, Paris : Hermès-Lavoisier.
  - Licoppe C., Draetta L. et Delanoë A., 2013, « Des smart grids au quantified self. Technologies réflexives et gouvernement par les traces », Intellectica, N° 59
  - Draetta L. et al., 2007, Ecologie des infrastructures numériques, Paris: Hermès Sciences.

Introduction

In 2011, in the ERIE special issue on "Ethics of Online Social Networks", we addressed privacy concerns with regards to online social network's use and news media's way of framing events without considering the ethical issues raised by such practices (Rizza, et al., 2011). At that time, our main concerns were related to users' expectations with regards to technology. We showed that social networks, and more generally main parts of emergent technologies, do not protect users from involuntary exposure due to either mistaken uses, or lack of control over published personal information. In this context, we considered that initiatives such as technologies embodying "ethics-by-design" or "privacy-by-design" concepts, as well as proposals for placing changes in regulation such as Poullet's (2010) ideas of Internet as virtual dwelling, were constituting relevant solutions to protect users and citizens from technologies and promote "ethical machines" (Sarah Spiekermann's blog 2014[1]).

Four years after, our concerns, threats and fears are coming from an even more "powerful" and ubiquitous Internet, called the 'Internet of things' (IoT). As presented in the call for papers the very concept of IoT was originally proposed in 1999 by Asthon to address the advent of RFID technology. But today IoT refers to various aspects: *"(i) the resulting global network interconnecting smart objects by means of extended internet technologies, (ii) the set of supporting technologies necessary to realize such a vision (including, e.g. RFIDs, sensors/actuators, machine-to-machine communication devices, etc.), and (iii) the ensemble of applications and services leveraging such technologies to open new business and market opportunities"* (Miorandi, Sicari, De Pellegrini, & Chlamtac, 2012). By 2020, 50 to 80 billion objects will be connected and will organize our daily life. Consequently, the IoT will be based on various mass-disseminated miniaturized technological devices. Combined, or not, with Big Data capabilities, this mass-dissemination of even more numerous and miniaturized smart objects will not come without a certain impact on our environment, health, and way of living (Draetta & Delanoë, 2012): it already questions our policy makers and us, as researchers.

In this position paper, we would like to promote the alternative approach positioned between the two extreme positions consisting in refusing any innovation or in adopting technology without questioning it. This approach has been brought and supported by researchers, entrepreneurs, and regulators for years and proposes a reflexive and responsible innovation (von Schomberg, 2013; 2011; 2007) based on a compromise between industrial and economic potentialities and a common respect of our human rights and values. More specifically, responsible research and innovation *"is a transparent, interactive process by which societal actors and innovators become mutually responsive to each other with a view to the (ethical) acceptability, sustainability and societal desirability of the innovation process and its marketable products (in order to allow a proper embedding of scientific and technological advances in our society)"* (von Schomberg, 2011, p. 9). Applied to the IoT context, we present the "silence of the chips right" as defined by Benhamou (2012; 2009) and we argue that it is timely, relevant and sustainable to face ethical challenges raised specifically by IoT when protecting citizen rights and values such as privacy, trust, social justice, autonomy and human agency. We believe the "silence of the chips" technical solution may support establishing an ethics of IoT embedded in the technology itself. Our position is not 'technocratic': we do not agree with discourses arguing technology can fix problems. Through the Responsible research and innovation approach we deeply believe and promote the idea that only human agency and user empowerment constitute a valid answer to the ethical, legal and social issues raised by technology and, in this particularly case, by IoT.

The paper is structured as followed: First part presents the main aspects of the literature review with regards to the ethical, legal and social concerns raised by IoT, as well as the responsible research and innovation approach. Second part addresses the present European context of IoT and RFID technologies deployment, and highlights the relevance of the "de-activation tag" technical solution in this context. In a third part, we focus on the "silence of the chip" right and show how, through the de-activation tag technical solution, it could contribute to the users' empowerment and protection from the ethical, legal and social issues as they have been emphasized in the state of the art. Last but not least, the discussion we bring in the fourth part puts

1 See : http://derstandard.at/r1326504100796/Die-ethische-Maschine

human agency and co-responsibility of societal actors and innovators at stake shedding light on why the ability to "shut down" the IoT chips should be implemented "by-design".

We conclude arguing that both the promotion of "the silence of the chips" right and its incorporation in IoT objects following an "ethics-by-design" approach, would allow us (as responsible citizens, researchers, regulators, etc.) to formulate an ethics for IoT, i.e. mainly focused on the ethical, legal and social challenges the IoT raises. In this context, the CIPRIoT research project is aiming at studying and – we hope so – stating the socio-technical viability of such concept.

State of the art

Ethical, legal and social concerns raised by the IoT

Technical papers in the field of IoT and ambient Intelligence underline the security and privacy issues raised by the deep penetration of technology in our everyday life associated with automation and remote interactions (e.g. Madeglia & Serbatini, 2010). Data collection, storage, mining and provision new capabilities combined with an increasing number of objects providing services, constitute so many possibilities of users' personal data collection (Ibid.).

Weber (2010) sheds light on the IoT security and privacy challenges from a legal point of view. To do so, he bases his analysis on the IoT architecture, i.e. an IT infrastructure composed by data communication tools (primarily RFID tagged objects) aiming at facilitating "communication" or "data flow" in a secure and reliable manner to provide a service. "Globality" – in the sense that the technology is used all over the world; "verticality" – due to the potential durability of the technical environment; "ubiquity" – referring to the technology possibility to be used ubiquitously to encompass persons, things, etc.; and "technicity" – due to the complexity of the tags, passive or active, and of the background device – characterize the IoT. These characteristics require new regulatory approaches guarantying privacy and security such as attacks' interception, data authentication, access control and guaranty of users' privacy (natural and legal persons). According to Weber (2010), IoT calls for a heterogeneous and differentiated legal framework: on one hand geographically limited national legislation does not seem appropriate; on the other hand, self-regulation may not be sufficient. Consequently, a solution could be the combination of a framework of key principals set at the international level combined with a more detailed regulation by the private sector (Ibid.).

As many others scholars, we consider that concerns about IoT go beyond privacy issues. IoT's event stresses more than ever a profiling logic of data identification, categorization and clustering without taking into consideration the context such data has been collected from (Hildebrandt & Gutwirth, 2007). Curvelo et al. (2014) warn against these "things" which collect and store data, forming a multiplicity of 'dossiers' on the user whereabouts that may be used in unexpected contexts. Consequently, the main question is not the "abuse" but the users' incapability to know whether and when their profiles are used or abused (Hildebrandt & Gutwirth, 2007).

In a hyper-connected era (Dewandre, 2013) where the promised interconnectivity through the IoT involves billions of smart human and non-human objects and transactions, "consent" may become an absurd concept (Curvelo, et al. 2014) and people may lose autonomy. According to Rizza (2014; 2006) the digital divide relies on several dimensions: access (to technology), digital competences in using in an accurate way technology to aim specific objectives, as well as supporting citizens' action. Some authors (e.g. Curvelo et al., 2014; Guimarães Pereira, Benessia, & Curvelo, 2013) consider IoT as an additional layer of divide between knowledgeable and skilled enough users to master the technology and to keep control, and disempowered users who do not question technology and do not protect themselves from abuse. Among the technological offer, empowered users are able to choose and even to drop-out a technology, whereas disempowered users become progressively more deskilled, disempowered and unknowledgeable. Consequently, IoT could compromise human

agency through what Curvelo et al. (2014) call "consent fatigue": the rising divides in this case are not exclusively related to lack of skills to deal with the complexity of interactions, but also to additional challenges in terms of knowledge production, skills development and empowerment.

Responsible research and innovation and privacy/ethics-by-design approaches

Scholars have long demonstrated the co-evolution of technology and society (e.g. Latour, 1992; Jasanoff, 1995). Feenberg (2010) articulates this as a democratic paradox: "the public is constituted by the technologies that bind it together but in turn it transforms the technologies that constitute it". However, von Schomberg (op. cit.) argues that the classical ethical theory and the conventional ethical practice do not address both aspects of unintentional consequences and collective decisions that should be taken into account while considering the issues of ethical responsibility in scientific and technological developments. Consequently, the interplay between IoT and privacy is part of a broader and long-debate (e.g. De Hert, 2009; Hildebrandt & Gutwirth, 2007).

De-activation tag technical solution in the European context

While the global market for RFID applications and IoT objects is expected to grow (Das & Harrop, 2014), an ongoing public debate is questioning the ethical, legal, and social implications of such ambivalent technology, whose technical features constitute its main challenges with regard to its co-construction with society (Draetta & Delanoë, op. cit.). For instance, the new European Norms and standards on RFID Privacy Impact Assessment and RFID Signage adopted last July[2], in completion with EU Data Protection rules and the Commission's 2009 recommendation on RFID, aim to help RFID and smart chips users and to protect European citizens/consumers while supporting at the same time this new market development. Nevertheless, surveillance - through traceability and technological opacity - and radiofrequencies emission when functioning, place RFID technology at the center of emerging controversies (Thiesse, 2007) with regards to major risks and concerns about privacy, public health and environmental impact.

Some initiatives are attempting to deal with current critique of technology contempt of ethical and societal concerns (e.g. Rizza, et al., 2011) by developing for instance technology embodying "ethics-by-design" or "privacy-by-design" paradigms (EC, 2010, p. 12), or by placing changes in regulation that currently implement traditional ethical concerns. In our context, a very practical example of this approach is the de-activation of RFID tags. Experiments are underway to test the possibility of de-activation tags attached to retailer goods after the sale. Indeed, RFID opponents consider that users' privacy infringement (individuals or enterprises) constitutes one of the main threats of RFID large-scale deployment due to RFID tags' invisibility and opacity. Conjointly, the social viability of smart tags' large-scale deployment strongly depends of public confidence with respect to the data protection the technology supports. So far, "killing" the chip was the only technical solution to protect users: once a product bought, the consumer is advised to destruct the tag initially placed in the product for inventory management or commercial reasons. Nevertheless, this solution does not fit the industrial opportunities chips could offer in terms of panel of services for users, and does not support IoT deployment. Consequently, instead of "killing" the chips, the systematic and reversible tag de-activation could constitute a sustainable technical and business solution.

The "silence of the chips" concept: towards an ethics(-by-design) for IoT?

Following the "deactivation tag" idea, Benhamou (op. cit.) presents the "silence of the chips right" as a means to establish trust between the different stakeholders: policy makers and industrials, on the one hand, users/citizens on the other hand. Indeed, the "silence of the chip" concept allows to face and master chips' specificities

2 European Commission, IP/14/889, 30/07/2014: http://europa.eu/rapid/press-release_IP-14-889_en.htm

such as their "durability", their "increasing numbers", and the data flow "opacity" they support. In this part, we then argue that the "silence of the chips right" (Ibid.) is timely, relevant and sustainable to face ethical challenges raised by IoT in terms of citizen rights and values protection such as privacy, trust, autonomy and human agency. By including "by-design" the "silence of the chip" concept in IoT, technology could support an ethics of IoT embedded in the technology itself.

Nevertheless, the 'silence of the chips' concept is at the center of a social-political and scientific controversy[3]. Some stakeholders suggest it is 'obsolete' due to the technical impossibility of erasing citizens' digital traces and due to "the paradigm shift" in the technology-society interactions (e.g. Ganascia, 2011). They propose to forget the "silence of the chips" concept and to adapt to the irrevocable pervasiveness of digital traces at the time when publishing and sharing one's own performance data have become the every-day life natural conditions of the "homo numericus" (Doueihi, 2008). To do so, they advocate a legal modification of the privacy concept as well as the promotion of citizens' resilience and empowerment.

Between the two extreme positions consisting in adopting this technocratic approach or in refusing any innovation and possibility of compromise, we think – as suggested by von Schomberg (op. cit.) - that responsible research and innovation constitutes another way-of-doing which would fully apply on the IoT context. By proposing a reflexive and responsible innovation based on a compromise between industrial and economic potentialities, and a common respect of our social contract's pillars such as Freedom, Education, Health, or Environment, and our human rights and values (Draetta, Musiani, Tessier, 2014), this approach would support us elaborating and applying a thoughtful response from both research and society to a field which is far from being just technical.

Following Benhamou's (op. cit.) idea, we consider the "silence of the chips right", i.e. the technological possibility to make the chip "silent" by de-activating it, a technical solution to both promote the IoT market development and support/protect "by-design" citizens' rights and human values.

Discussion: co-responsibility and human agency at stake

The state of the art allows to frame the ethical legal and social concerns related to the IoT advent. From a technical point of view, the increasing number of IoT objects combined to their ubiquity, their durability and complexity (Weber, op. cit.) raises security challenges to preserve users' privacy (Madeglia & Serbatini, op. cit.; Weber, Ibid.). IoT constitutes an additional technical capability in collecting, storing and processing users' personal data for economic and commercial purposes. But, overall, the IoT data-flow opacity does not allow users controlling their own data. As suggested by Curvelo, et al. (op. cit.) and Hildebrandt & Gutwirth (op.cit.), in the IoT context users are not protected from any abuse due to their incapability to know whether, when and where their data is used.

In this context, we claim that, so far, IoT has been implemented in a technocratic way disempowering users from their capability to question, choose or even drop out the technology. So far, in this 'new' market the IoT constitutes, IoT objects are proposed and sold to fix everyday 'little' problems citizens are facing: everything can be monitored through sensors to simplify users' life. As an illustration, during the Leroy Merlin workshop "Inhabitants, housing and digital data: towards a new and controlled porosity of the housing borders?"[4], Blandine Calcio Gaudino shed light on the simplistic way elderly is explained how IoT is implemented in their own home and is asked to not being worried about anything since sensors will "take care" of "everything". We consider that present technocratic discourses coming with the IoT implementation simplify the IoT complex

3 See: The Observatory for Responsible Innovation workshop's follow-up on "La RFID à l'épreuve de l'innovation responsable", 14/03/2014: http://www.debatinginnovation.org/?q=node/116

4 Leroy Merlin third conference on housing - Workshop "inhabitants, housing and digital data: towards a new and controlled porosity of the housing borders?" – speakers Calcio Gaudino B., Desbiey O., Rizza C., & Sadde G., 11/02/2015: http://leroymerlinsource.fr/savoirs-de-l-habitat/chez-soi/assise-de-lhabitat-2014/

reality and contribute at the same time to disempower users, expending without their own knowledge the digital divide.

In some way, the new European Norms and standards on RFID Privacy Impact Assessment and RFID Signage (July 2014, op. cit.) constitutes a first attempt to make aware citizens/users about the RFID or IoT chips presence in an object. This is not about modifying the legal definition of privacy in order to "respond" to the new and irrevocable technical capability in tracing and profiling users, but it is all about making transparent what was not anymore visible in order to empower users and to protect them.

In this context, we argue that, by giving the possibility to users to make silent the chips embedded into the technologies or objects they are using or owning, the "silence of the chip" concept makes possible – again – human agency. Indeed, the "silence of the chip" concept allows users to give consent to their data's transmission/collection – responding to the first privacy concern raised in the literature review. But more specifically, the silence of the chip concept induces users' awareness about the presence of a 'smart' chip in the object they are using. Consequently, it makes visible processes which were no longer transparent. Doing so, it contributes to a better understanding on what is going on through the IoT object or technology, reducing IoT use's complexity but, first of all, preventing users from "abuse". Second, giving users the ability of silencing the chip requires them to assess opportunities of activating or de-activating tags with regards to their uses and needs: they are not anymore passive in front of a technology managing their environment and "fixing" their problems. Consequently, the "silence of the chip" concept also addresses concerns related to users' autonomy. It supports users' empowerment with regards to IoT technology.

Last but not least, following the responsible research and innovation approach (von Schomberg, op. cit.), we would like to insist on societal actors' and innovators' co-responsibility when developing and implementing a technology. "By-design" a technology should embed the human values we (as innovators, researchers, entrepreneurs, policy makers, citizens/users) would like to defend and promote in our society: "by-design" the IoT should respect and promote user's privacy, autonomy, social justice, etc. But, as we have already claimed, we also deeply consider that a technology cannot fix users' problems, cannot replace "human" action. If sensors can 'allow' elderly to stay home instead of being hospitalized, an elderly cannot be responsible in case something happens during a moment the chip would have been switched off: technology, in this case sensors, has to be implemented to support a team helping an elderly to stay home, but under no circumstances has to substitute human agency. Another relevant illustration is the French case emerged in the early 2000 when clinics asked future parents to sign a disclaimer if they refused their newborns were equipped with electronic tagging to prevent any rapt. Users and stakeholders (social actors, policy makers, entrepreneurs, etc.) are co-responsible when implementing or using a technology in a specific context and use. Users' empowerment cannot be a motive of releasing stakeholders from their responsibility. "By-design" giving to users the means to question technology and to act (through the de-activation/re-activation tag possibility) will make IoT ethically acceptable and socially desirable[5].

Conclusion

Studying online social networks, Walther (2011) has shed light on Internet online users' misplaced presumption: 1) that online behaviors were private; 2) that the Internet nature was incommensurate with privacy as we have known it; and 3) that private online "conversations" remained as such. At that time, already, we agreed with the idea that Internet and emergent technology were not protecting their users, and that technology should "by-design" include concepts, values, we would like to promote and protect. Four years after, the "hybridation" of real and virtual worlds through the IoT constitutes again more than ever a threat for these values – e.g. privacy, autonomy, social justice, human agency. More than ever, a responsible research and innovation promoting technology embedding by design our human rights and values is timeline. In some way, the silence of

5 Please note that von Schomberg's definition of responsible research and innovation also includes a "sustainable" dimension we have not taken into consideration in this paper.

the chip concept based on the deactivation tag technical solution would support what the new European Norms and standards on RFID Privacy Impact Assessment and RFID Signage (supra) is attempting to implement: protecting citizens' privacy and raising their awareness while promoting the European RFID and IoT market development. This is why, in a shared co-responsible approach of innovation, we consider that both promoting "the silence of the chips" concept and incorporating it through the de-activation tag technical possibility in IoT technologies following an "ethics-by-design" approach, would allow us (as responsible citizens, researchers, regulators, etc.) to formulate an ethics for IoT, i.e. mainly focused on the ethical, legal and social challenges it raises.

In this context, we started last January, a sociological research project in order to assess the socio-technical viability of the "silence of the chips" concept in RFID systems for IoT contexts. The CIPRIoT project[6] aims at:

1) Bringing elements of scientific knowledge in the field of hybridization phenomena between technological innovation, social innovation and value creation;
2) Proposing to policy makers and industry recommendations and guidelines in order to understand societal implications of RFID and IoT technologies, as well as promote a responsible and sustainable innovation based on users' protection through an "ethics-by-design" R&D.

To do so, we are conjointly studying the social demand and the operational viability of the "silence of the chip" concept through three analysis levels: 1) macro level: scientific and socio-political controversies as they emerge in the scientific and mainstream literatures as well as digital spaces; 2) Meso level: industrial R&D projects in the RFID and IoT fields through a documentary analysis and interviews with industrials project leaders; 3) Micro level: "smart home" use case.

References

Benhamou, B. 2012. Les mutations économiques, sociales et politiques de l'internet des objets. Cahiers Français – Documentation Française, 4 décembre 2012.

Benhamou, B. 2009. Internet des objets. Défis technologiques, économiques et politiques, Revue Esprit, Mars-Avril.

Curvelo P. et al. 2014. The constitution of the hybrid world: EU Scientific & political report. Publications Office of the European Union.

Das R. and Harrop, P. 2014. "RFID Forecasts, Players and Opportunities 2014-2024", IDTechEx report, July: http://www.idtechex.com/research/reports/rfid-forecasts-players-and-opportunities-2014-2024-000368.asp

Dewandre, N. 2013. Rethinking the Human Condition in a Hyperconnected Era, The Online Manifesto, DG Connect, European Commission.

Doueihi M. 2008, La Grande conversion numérique, Paris : Le Seuil.

Draetta L. et Delanoë A., 2012, RFID une technologie controversée. Ethnographie de la construction sociale du risque, Paris : Hermès-Lavoisier

Draetta L., Musiani F., Tessier D., 2014, RFID and responsible innovation: towards a positive compromise?, Debating Innovation, Vol. 4(1): 9-15.

European Commission, 2010. "A comprehensive approach on personal data protection in the European Union", COM(2010) 609 final, Brussels, 4.11.2010

Feenberg A. 2010. Between reason and experience: essays in technology and modernity. Cambridge MA: The MIT Press.

6 "Use information, hide the trace: CItizen's Privacy in RFID and IoT contexts. Exploratory study for the socio-technical viability of the 'silence of the chips' concept " Research project funded by the Foundation Mines-Telecom.

Ganascia J.-G. 2011. The new ethical trilemma: Security, privacy and transparency, Comptes Rendus Physique, vol. 12 (7), pp. 684-692.

Guimarães Pereira A., Benessia A., & Curvelo P. 2009. Agency in the Internet of Things, JRC Scientific and Policy Report, Publications Office of the European Union.

Hildebrandt M. and Gutwirth S. (Eds). 2007. Profiling the European Citizen. Cross-disciplinary perspectives, www.fidis.net

Jasanoff S. 1995. Science at the Bar: Law, Science, and Technology in America, a Twentieth Century Fund book, Cambridge, MA: Harvard University Press.

Latour B. 1992. Where are the Missing Masses? The Sociology of a Few Mundane Artifacts, in: Shaping Technology/Building Society: Studies in Sociotechnical Change, Bijker, W.E. and Law, J. (Eds), MIT Press, USA, 225-258.

Madeglia, C.M. & Serbatini, A. 2010. An overview of privacy and security issues in the Internet of things. In: D. giusto et al. (eds.), The Internet of things: 20th Tyrrhenian Workshop on digital communications, DOI 10.1007/978-1-4419-1674_38

Miorandi, D., Sicari, S., De Pellegrini, F., & Chlamtac, I. 2012. Internet of things: vision, applications and research challenges. Ad Hoc Networks. http://dx.doi.org/10.1016/j.adhoc.2012.02.016

Poullet Y. 2010. About the E-Privacy Directive: Towards a Third Generation of Data Protection Legislation? In: Data Protection in a Profiled World, Springer Netherlands: 3-30.

Rizza C. et al. 2011. Interrogating privacy in the digital society: media narratives after 2 cases, International Journal of Information Ethics, vol. 16; p. 6-17.

Rizza C. 2014. Digital divide. In: Alex C, Michalos, Encyclopedia of Quality of Life and Well-Being Research. p. 1619-1621, DORDRECHT: Springer.

Thiesse, F. (2007), "RFID, privacy and the perception of risk: A strategic framework", The Journal of Strategic Information Systems, 16(2): 214–232.

Von Schomberg R. 2007. From the ethics of technology towards an ethics of knowledge policy/knowledge assessment. Publication series of the Governance and Ethics unit of DG Research. Brussels, European Commission.

Von Schomberg R. 2011. Prospects for Technology Assessment in a framework of responsible research and innovation. In: M. Dusseldorp and R. Beecroft (eds). Technikfolgen abschätzen lehren: Bildungspotenziale transdisziplinärer Methode, p. 39-61, Wiesbaden: Springer VS.

Von Schomberg R. 2013. A vision of Responsible Research and Innovation, in Owen R. et al. (eds.), Responsible Innovation, London: Wiley, 51-74.

Walther, J. B. (2011). Introduction to Privacy Online. Privacy Online: Perspectives on Privacy and Self-disclosure in the Social Web. S. Trepte and L. Reinecke. Heidelberg, Springer: 3-8.

Weber, R.H. 2010. Internet of Things – New security and privacy challenges, computer Law and security Review 26(2010) pp. 23-30.

Soenke Zehle:

Reclaiming the Ambient Commons: Strategies of Depletion Design in the Subjective Economy

Abstract:

The vision of an internet of things, increasingly considered in the context of the "internet of everything", calls for an ethics of technology driven less by the philosophical search for the essence of technology than by a transversal curiosity regarding processes of constitution. If growing interest in enhanced and expanded media literacy approaches facilitates ethical reflection, the scope of such reflection is related to the extent of our attention to and awareness of the immanence of our agency, our capacity for relation in machinic assemblages that structure and sustain our communicative existences far beyond the sphere of signification. While the positions from which such reflection occurs are necessarily multiple, we can still respond to the distribution of agency with an aggregation of responsibility and the creation of a commons with greater attention to the vastness of the spatial and temporal scales of our situation. The idea of depletion design is both a concrete set of design strategies and an attempt to establish an experimental institutional object to facilitate and frame such ethico-aesthetic practice, an architecture for commoning that situates and affirms our ethical agency under the conditions of mediation.

Agenda:

Author:

Dr. Soenke Zehle:

- xm:lab – Experimental Media Lab, Academy of Fine Arts Saar, Saarbruecken, Germany
- ☎ + 49 - 681 – 92651 - 150 , ✉ s.zehle@xmlab.org, 💻 www.xmlab.org/about/people/zehle
- Relevant publications:
  - Documenting Depletion: Of Algorithmic Machines, Experience Streams, and Plastic People. In: Richard Maxwell, Jon Raundalen, and Nina Lager Vesterberg (eds), Media and the Ecological Crisis, London: Routledge 2015, pp. 52-68.
  - Transcultural Media Studies. In: George Ritzer (ed), The Wiley-Blackwell Encyclopedia of Globalization, Chichester, West Sussex; Malden, MA: Wiley Blackwell 2012.
  - Rossiter, Ned; Zehle, Soenke: Data Politics and Infrastructural Design: Between Cybernetic Mediation and Terminal Subjectivity. Special Issue: Datafied Research. APRJA 4.1 (2015).
  - Rossiter, Ned; Zehle, Soenke: Experience Machines, Sociologia del Lavoro 133 (2014), pp. 111-133.
  - Wiedemann, Carolin; Zehle, Soenke (eds): Depletion Design: A Glossary of Network Ecologies. Theory on Demand #8. Amsterdam: Institute of Network Cultures, 2012.

ISSN 1614-1687

The vision of an internet of things, increasingly considered in the context of the "internet of everything", calls for an ethics of technology driven less by the philosophical search for the essence of technology than by a transversal curiosity regarding processes of constitution. If growing interest in enhanced and expanded media literacy approaches facilitates ethical reflection, the scope of such reflection is related to the extent of our attention to and awareness of the immanence of our agency, our capacity for relation in the machinic assemblages that structure and sustain our communicative existences far beyond the sphere of signification. And while the positions in which such reflection occurs are necessarily multiple, we can still respond to the distribution of agency with an aggregation of responsibility and the creation of a commons with greater attention to the vastness of the spatial and temporal scales of our situation, preceding and exceeding the scales of venture capital and innovation governance. The idea of depletion design is both a concrete set of design strategies and an attempt to establish an experimental institutional object to facilitate and frame such ethico-aesthetic practice, an architecture for commoning that situates and affirms our ethical agency under the conditions of mediation.

I. Metaphors of Mediation

"Understanding the nature of infrastructural work involves unfolding the political, ethical, and social choices that have been made throughout its development," making infrastructures "a fundamentally *relational* concept".[1] From the early days of vending machines sending status reports via dial-up modems to the sensor networks in an "industrial internet" of self-optimizing assets and operations, m2m communication is an integral element of an internet of things.[2] "M2M" no longer stands only for the many-to-many forms of communication facilitated by peer-to-peer logics, but also for the machine-to-machine communication among edge devices linked in cloud-based networks. Supported by "sensor driven decision analytics", smart objects make decisions, even if the initial degree of object agency may remain far more modest than anticipated in ambitious visions of artificial intelligence.[3] And while the computational capacity of individual devices is rather limited, the prospect of m2m communication on a massive scale already drives the design of network infrastructures and regulatory frameworks that can structure and sustain the (self-)organization of the emergent machinic multitude at the heart of a new dynamic of mediation.

To focus on the dynamic of mediation is to acknowledge the structural transformation of the technical object and take its disperal into technical networks as analytical point of departure: "The concept of the technical object has itself become, because of its fundamental environmentalization, problematic, if not obsolete ... In contrast to the ever-repeated refrain of a new immediacy, into which we (re)enter in the age of ubiquitous computing, ubiquitous media, intelligent environments, and so on, we are in fact now dealing with the absolute prioritization of mediation."[4] To assess the ethical stakes of mediation, we will need to comprehend its infrastructural relationalities, the modes of relation through which it structures our communicative socialities and imagines individual and collective engagement. Given the central role metaphors play in the way we come to terms with our experience, one way to begin such an assessment is to look for new metaphors, metaphors drawn directly from the material infrastructures of mediation.[5] The two following examples – the data fabric and the zero-bandgap semiconductor – offer a way to comprehend two key registers of the "infrastructural relationality" of mediation: the becoming-topological of culture, and the seamlessness of surfaces that not only envelop us but literally implicate us in the constitution of our material environments.

1 Bowker, Geoffrey C.; Miller, Florence; Ribes, David: Toward Information Infrastructure Studies. Italics in original.

2 On GE's vision of an 'industrial internet' ('Big Iron meets Big Data'), see http://www.gesoftware.com, also Lansiti, Marco; Lakhani, Karim T.: Digital Ubiquity.

3 McKinsey analysts describe IoT value chains in terms of 'sensor driven decision analytics', see Chui, Michael; Loeffler, Markus; Roberts, Roger: The Internet of Things. What defines an IoT is that many of these decisions are made by machines.

4 Hoerl, Erich: A Thousand Ecologies. 124.

5 Lakoff, George; Johnson, Mark: Metaphors We Live By.

ISSN 1614-1687

In assessments of the cost of increasing the connective capacities of emerging human-nonhuman collectives, attention has shifted from end-user devices (conflict minerals, e-waste, occupational health and safety across the supply chain) to network infrastructures, including datacenters.[6] Exemplifying a trend toward software-defined networks, Facebook's new data center topology follows a fabric rather than a cluster model: "Fabric offers a multitude of equal paths between any points on the network, making individual circuits and devices unimportant – such a network is able to survive multiple simultaneous component failures with no impact."[7] The new generation of software-defined hyperscale networks is designed to facilitate "infrastructure as a service" approaches: "In the SDN architecture, the control and data planes are decoupled, network intelligence and state are logically centralized, and the underlying network infrastructure is abstracted from the applications".[8] A hierarchical network design (tiers of switches organized in a tree structure) "made sense when client-server computing was dominant, but such a static architecture is ill-suited to the dynamic computing and storage needs of today's enterprise data centers, campuses, and carrier environments".[9] Instead, SDNs are in principle programmable "by operators, enterprises, independent software vendors, and users (not just equipment manufacturers) using common programming environments."[10] Driven by changes in data management that call for scalable, dynamically reconfigurable infrastructures, the notion of "data fabrics" also recalls the historical link between mechanical looms and the origins of machinic computation.[11]

The notion of data fabrics reminds us that software is one of the dimensions in the becoming-topological of culture: „Just as adding a new dimension adds a new coordinate to every point in space, 'adding' software to culture changes the identity of everything that a culture is made from".[12] Software reconfigures the space of experience. The haptic qualities we imagine a fabric to have relate these scalable infrastructures to the proliferation of surfaces of sensation. For Cecilia Lury et al, that "contemporary culture is itself coming to display a proliferation of surfaces that *behave topologically*" becomes apparent in the way "the "borders" or „frames" of mirrors, windows, screens and interfaces have become surfaces of sensation themselves by operating the opposition between inside and outside in a dynamic re-making of relations to each other ... the frames of mediation have come to produce topological spaces".[13] As the number of interfaces grows in the wake of smart urbanization schemes based on internet-of-things technologies, for example, these interfaces don't simply provide access or information, they are involved (and involve us) in processes of mediation.

Popular visions of an informatization of urban environments take the technological vision of an active city further, envisioning the employment of sensor networks to create sentient spaces. For Mark Shephard, "To understand the implications of this folding of people, street, and data onto each other requires thinking about space in visual ways, where formal geometry and material articulation become less relevant than the topologies of networked information systems and their intersection with the socio-spatial practices of daily life".[14] While urbanists adopt urban experience design approaches to explore new relationships between users and informatized infrastructures, the growing interest in "smart" cities also intensifies conflicts related to the enmeshment

6 When the University of Delaware decided against the construction of a new data center in 2014, it did so in because of community opposition to the environmental impact of the 280 megawatt power plant meant to power the data center. http://www.datacenters.com/news/featured/plug-pulled-on-tdcs-delaware-data-center-and-power-plant/.

7 Andreyev, Alex: Introducing data center fabric.

8 See Open Network Foundation: Software-Defined Networking.

9 Ibid. 3.

10 Ibid. Future Facilities offers a popular data center modeling software, see http://www.6sigmadcx.com/.

11 On the Jacquard loom that inspired Charles Babbage's Analytical Machine, see Manovich, Lev: The Language of New Media; Essinger, James: Jacquard's Web.

12 Manovich, Lev: Software is the Message. 80.

13 Lury, Celia; Parisi, Luciana; Terranova, Tiziana: Introduction: The Becoming Topological of Culture. 9. Emphasis in the original.

14 Shepard, Mark: Toward the Sentient City. 21.

of such sentient spaces in the extractive economies of capture – the public and private surveillance of our communicative practices to establish data-driven models of governance and growth.[15]

The vision of everyday objects as active agents in the collection and redistribution of data is driven in part by materials research. With the help of new (single-layer) materials, suggests Tomas Palacios of MIT/MTL's Center for Graphene Devices and 2D Systems, "everything around us will be able to convert itself into a display on demand", including the design of smart dust.[16] As a zero-gap carbon monolayer semiconductor (essentially a one-atom thick layer of graphite), Graphene does not possess an inherent band gap, i.e. an energy range in which various states of electron flow can exist, making it difficult to harness its conductive properties for any application that requires an on/off capability. So the gap is what has to be engineered for these constituent elements of infrastructures of mediation to operate.[17] The material's properties offer a powerful metaphor - of always-on worlds, of uninterruptible faster-than-ever flows, of infrastructures comprehensible only to a molecular vision. It also illustrates that a new era of connectivity requires new materials - or a new sense of the materialities that already exist, of the role they play in our logics of existentialization and new economies of capture. Together with the notion of data fabrics of software-defined computational folds, the "gapless" material helps comprehend our implication in the "infrastructural relationalities" of mediation.

II. Strategies of Depletion Design

Depletion is where the common begins, in sites to which no one lays claims anymore because they have been exhausted. Exhaustion leaves fragments, ruins, waste, it is what comes after production, after use, after work. Depletion offers a way to map a terrain, to delineate a horizon from within which to articulate a politics of depletion. Traversing an open semantic field to sketch a cartography of the political, the use of depletion as a shifting vantage point to survey sites and situations of physical and psychosocial exhaustion opens up new modes of relation, suggesting that we translate shared (semantic) properties into technologies of the common as we connect the exhaustion of natural resources to the exhaustion that follows from the distribution of life and labor across real-time networks.[18] The question of depletion design is a question of agency under the condition of depletion: how do we engage with the dynamics of exhaustion, how do we create interfaces for engagement, how do we structure processes of decision-making.

„The commons is invisible until it is lost."[19] Designed to co-develop and facilitate practice-based projects in the spirit of depletion design, xm:lab's School of Things provides a setting to critically engage the vision and consequences of a world of informatized objects.[20] Because it is driven by the idea of a technological commons that strives to enable and maintain autonomous forms of use, the depletion design approach explored in the School of Things necessarily includes attention to strategies of enclosure-by-design that limit the scope of use afforded by many, if not most digital objects and infrastructures. Deliberately disallowing acts of commoning through reappropriation and reuse, such strategies include the specifications of hardware and software as well as the standards and protocols that govern the operation of digital technologies. All projects revolve around

15 See, for example, Singapore's „Smart Nation" initiative, where the discourses of smart urbanization are integral to national development roadmaps. http://www.ida.gov.sg/Infocomm-Landscape/Smart-Nation-Vision/.

16 Colapinto, John: Material Question. The design of smart dust captured the imagination of military researchers at RAND in the early 1990s and briefly reappeared in Gartner's 2013 Hype Cycle Report; smart dust (here: swarms of nano-robots) already appears as collective machinic protagonist in Stanislaw Lem's 1964 (English: 1973) science fiction novel The Invincible, a literary thought experiment that explores the "necroevolution" of self-organizing non-living matter.

17 The properties of Graphene (the strongest material ever tested) have attracted substantial research subsidies. See, for example, the Graphene Flagship, the EU's largest research project to date (1 billion €) http://graphene-flagship.eu/, the MIT/MTL Center for http://www-mtl.mit.edu/wpmu/graphene/, as well as journals addressing the needs of a new generation of materials researchers-turned-science-entrepreneurs, see http://iopscience.iop.org/2053-1613/.

18 Wiedemann, Carolin; Zehle, Soenke: Depletion Design.

19 Linebaugh, Peter: Stop Thief! The Commons, Enclosures, and Resistance. 14.

20 http://www.schoolofthings.org/.

the core principle of playful experimentation with concrete possibilities of intervening and participating in the aesthetic and technological design of such a "smart" world, (re)opening these technologies to individual and collective reappropriation.

Like other educational efforts across the global maker movement, it is sustained by the enthusiastic embrace of new forms of embodied education and procedural media literacy that shift the focus and perspective of analysis toward the immersive stance of comprehension-through-creation.[21] Shared across hackers, makers, and creative coders, such an ethico-aesthetic stance counters the technodeterminist visions of predictive politics, economies of capture, and behaviorist governance made possible by an internet of things. Rather than constituting a retreat into the nostalgic terms of digital craft, it is motivated by an ethos of making that involves an active engagement with algorithmic cultures, a parametric politics of collaborative creation, a technology of play to change the rules of the networking game. At the same time, it is aware of the limits of generalizing prototyping approaches into a neo-industrial development framework, of replacing public support with the logic of venture capital, and of turning "making" into an all-encompassing paradigm of social innovation that crowds out autonomous and more antagonistic socialities.[22]

While it is (comparatively) easy to comprehend how different licensing schemes for hardware and software constrain or expand the agency of users choosing to work with a specific set of digital technologies, it is more difficult to see how the collection of data in automated "smart" systems affects such freedoms of use, especially when these dynamics are designed to disappear from view.[23] One strategy to keep the increasing number of real-time flows manageable has been the shift toward natural interfaces that require less and less explicit attention. The less our interaction with such a world of ambient intelligence is based on prior knowledge, structured searches, and deliberate choices, the more our environments have to know about us, our location, our preferences, our histories of interaction: we are, by definition, not only on the terrain of discourse and deliberation but of experience, of affect, of sensation.[24] Yet whereas it is the depletion of a commons that makes us aware of its existence, it is difficult to make this loss visible in the case of algorithmic processes operating beyond our scales of perception.[25] One way to think about life and labor in the sentient spaces of our smart cities (whose semiotic machines are fueled by our data exhaust) is to imagine the sphere of atmospheric media as an "ambient commons".[26] The tradition of commoning, of reproducing resources as shareable and in principle subject to collaborative forms of governance, offers rich resources to comprehend the enclosure of experience.[27] The notion of ambience captures both the characteristics and the consequences of the becoming-ubiquitous of information and communication technologies, enveloping us in the multi-layered fabrics of a subjective economy in which every expression, every act of relation can be stored and retrieved as potential element in processes of valorization.

21 Blikstein, Paulo: Digital Fabrication and 'Making' in Education; Bogost, Ian: Procedural Literacy; Halverson, Erica Rosenfeld; Sheridan, Kimberly M.: The Maker Movement in Education; Honey, Margaret; Kanter, David: Design, Make, Play; Schoen, Sandra; Ebner, Martin; Kumar, Swapna: The Maker Movement; Sharples, Mike et al: Innovating Pedagogy; Streeck, Juergen; Goodwin, Charles; LeBaron, Curtis (eds): Embodied Interaction.

22 Fonseca, Felipe: Repair Culture.

23 For conceptualizations of a „data commons" see Yakowitz, Jane: Tragedy of the Data Commons; Zuiderwijk, Anneke; Janssen, Marijn; Davis, Chris: Innovation with open data; Dragona, Daphne: Counter-Infrastructures.

24 Hansen, Mark B.N.: Feed-Forward.

25 Zehle, Soenke: Documenting Depletion.

26 McCullough, Malcolm: Ambient Commons.

27 Ostrom, Elinor: Governing the Commons; Ostrom, Elinor; Hess, Charlotte: Understanding Knowledge as a Commons; Linebaugh, Peter: The Magna Carta Manifesto.

III. Machinic Matrices of Experience

To better comprehend communication infrastructures as "matrices of experience", it does not make sense to reestablish the dichotomy between machines (technical objects) and non-machines (human beings).[28] In his brief history of the 'Guattari-Effect', Eric Alliez recalls that "Guattari-Deleuze had warned us: the machine is not a metaphorical figure."[29] In his own survey of the term machine, Gerald Raunig recounts the history of a disappearance. Whereas „the commonplace concept of the machine … refers to a technical object, which can be precisely determined in its physical demarcation and seclusion, as well as in its usability for a purpose, … the machine was once conceptualized quite differently, namely as a complex composition and as an assemblage that specifically could not be grasped and defined through its utilization".[30] A delineation of object/subject boundaries alone cannot grasp the distributed actuality of machinic multiplicity, comprehend what is happening to us - our agency, our capacity for relation.[31] If media becomes machinic, so do we.

For Maurizio Lazzarato, "the component parts of subjectivity – intelligence, affects, sensations, cognition, memory, physical force – are components whose synthesis lies in the assemblage or process, and not in the person".[32] A subjective economy is designed to exploit these component parts: "Subjective economy means subjectivity existing for the machine, subjective components as functions of enslavement which activates pre-personal, pre-cognitive, and pre-verbal forces (perception, sense, affect, desire) as well as supra-personal forces (machinic, social, linguistic, economic) which go beyond the subject: it involves neither representation nor consciousness, it is machinic."[33] He conceptualizes the machine as something other than a tool, "which makes the machine an extension and projection of the human being."[34] Machines are assemblages, operating below and above our levels of cognition and perception: "*In a machine-centric world, in order to speak, smell, and act, we are of a piece with machines and asignifying semiotics*."[35] As users whose agency is enmeshed in sensor networks, we are on the terrain of an a-signifying semiotics of sensation.[36]

In his *Summa Technologiae*, Stanislaw Lem anticipated the need of networked societies overwhelmed by information to overcome such an „information barrier" through the automation of cognition.[37] Recalling Lem's vision, N. Katherine Hayles reflects on the „scope and essence of interpretation" and notes that to acknowledge that interpretation „applies to information flows as well as to questions about the relations of human selves to the world", we need to approach thought and cognition as distinct processes: „while all thinking is cognition, not all cognition is thinking".[38] What she terms „nonconscious cognition" is not, however, a capacity of computational objects, but „operates across and within the full spectrum of cognitive agents: humans, animals, and technical devices."[39] And whereas „material processes operating on their own rather than as part of a complex

28 Foucault, Michel: The Government of Self and Others. 41.

29 Alliez, Eric: The Cause of the Guattari Effect. 96.

30 Raunig, Gerald: A Thousand Machines.

31 Lazzarato, Maurizio: Exiting Language.

32 Future Art Base: Power at the End of the Economy.

33 Ibid.

34 Lazzarato, Maurizio: Signs and Machines. 80, 81.

35 Ibid. 88.

36 Alliez: „if there is no real distinction between expression and content, we are in a semiotics of intensities. And surely the fundamental category of Félix is the idea of an a-signifying semiotics" (ibid.). On the concept of a semiotics of intensities, also see Alliez, Eric: Diagrammatic Agency Versus Aesthetic Regime of Contemporary Art.

37 Stanislaw Lem, Summa Technologiae, trans. Joanna Zylinska, Minneapolis: University of Minnesota Press, 2014. In a chapter dedicated to „intellectronics" (artficial intelligence), Lem describes the options in addressing the information barrier in terms of a „game of information"; with the evolution of „automatic gnosis" (for Lem, the winning scenario), information can act on other information without human involvement.

38 Hayles, N. Katherine: Cognition Everywhere. 218, 201.

39 Ibid. 202.

adaptive system do not demonstrate emergence, adaptation, or complexity", the delineation of boundaries between „conscious thinking, nonconscious cognition, and material processes" is a matter of debate rather than mere distinction.[40] Reflecting on nonconscious cognition as a discrete capacity distributed across a wide variety of agents, Hayles also draws attention to the costs of consciousness. They include its belatedness, i.e. the „missing half second" that separates the initiation of neural activity and conscious awareness, which can be exploited by new forms of nonconscious cognition in advertizing or the algorithmic trading in near-real time financial markets. But perhaps more importantly, such costs include the anthropocentric bias consciousness establishes: „The same faculty that makes us aware of ourselves as selves also partially blinds us to the complexity of the biological, social, and technological systems in which we are embedded."[41] Attention to nonconscious cognition not only leads us to realize that „an object need not be alive or conscious in order to function as a cognitive agent", but to greater awareness of this complexity.[42] And if the new commons are ambient, we need ambient methodologies to create new forms of commoning – methodologies that comprehend the "infrastructural relationalities" of mediation and the dynamic of semi-autonomous systems operating in the subjective economy.

IV. Reclaiming the Ambient Commons

As informatization expands to include a vast array of everyday objects as active agents in technological networks, it is the ambient commons of our space of experience that is subject to new forms of enclosure. Which is why, „if ‚commoning' has any meaning, it must be the production of ourselves as a common subject", as the practices of creating and recreating the commons necessarily involve processes of individual and collective self-constitution.[43] As more and more corporate actors intervene in the space of self-relation, offering infrastructures and operating systems to organize the distribution of life and labor across the complex topologies of our algorithmic cultures, we need a much better sense of how these processes shape our modes and capacities for relation, of how we can come to terms with the enclosure of this space of experience, what role we envision for ourselves in stories of commoning.

Johanna Zylinska has sketched a *Minimal Ethics for the Anthropocene*, defined as „a set of actions we can undertake once we have intuitively grasped this constant movement of life, of which we are part, and then turned to our compromised and imperfect faculty of reason - which is perhaps primarily a storytelling faculty - in order to tell better stories about life in the universe, and about life (and death) *of* the universe".[44] For her, "ethics is a historically contingent human mode of becoming in the world, of becoming different from the world, and of narrating and taking responsibility for the nature of this difference", and she describes "ethics as a relatively narrow cultural practice, worked out by humans across history, as a form of regulating ways of co-existing and co-emerging with others. This cultural practice also involves providing an account - verbally, experientially, or aesthetically - of these processes of co-existence and co-emergence."[45] Understood both as a concrete design strategy and an experimental institution, depletion design involves the elaboration of an architecture for storytelling from within such an ethical horizon. What such stories share is the sense that their ethical impact does not derive from the construction of ethical agency that severs the human from its machinic contexts, but precisely from an acknowledgment of the irreducible machinic constitution of our capacities for communication and relation.

For Bruno Latour, here we will already have to make a decision, and it is a decision about the temporal horizon from within which we engage these questions: "Between matter and materiality, then, we have to choose. …

40 Ibid. 202.

41 ibid. 204-5.

42 Ibid. 216.

43 Federici, Silvia: Revolution at Point Zero. 145.

44 Zylinski, Johanna: Minimal Ethics for the Anthropocene. 46.

45 Ibid. 93, 92.

Matter is produced by letting time flow from the past to the present via a strange definition of causality; materiality is produced by letting time flow from the future to the present, with a realistic definition of the many occasions through which agencies are being discovered."[46] The comprehension of agency does not proceed by way of reaggregating their dispersion: "The point of living in the epoch of the Anthropocene is that all agents share the same shape-changing destiny, a destiny that cannot be followed, documented, told, and represented by using any of the older traits associated with subjectivity or objectivity. Far from trying to "reconcile" or "combine" nature and society, the task, the crucial political task, is on the contrary to distribute agency as far and in as differentiated a way as possible - until, that is, we have thoroughly lost any relation between those two concepts of object and subject that are no longer of any interest any more except in a patrimonial sense."[47] Instead, we need to imagine the implications of a radical distribution of agency.

The way we tell stories is a a key element in our decisions regarding the creation and (re)use of old and new technologies. While interactive and immersive aesthetics have already come to play a central role in the exploration of storytelling futures, storytelling continues to draw on the complexity and richness of existing practices. Rather than stressing the compositional dimension of narrative constitution, the conceptual and metaphorical focus on architectures shifts analytical attention to the infrastructural implications of storytelling, i.e. quite literally the way in which stories fold / unfold across the topologies of experience: "It is easy to see why it will be utterly impossible to tell our common geostory without all of us - novelists, generals, en- gineers, scientists, politicians, activists, and citizens - getting closer and closer within such a common trading zone."[48] The gestures of reappropriation that are the core of depletion design strategies are key elements in comprehending the potentialities of technologies, of exploring their constitution, of gauging their impact – and of creating matters of concern: "Traditionally, politics needs to endow its citizens with some capacity of speech, some degree of autonomy, and some degree of liberty. But it also needs to associate these citizens with their matters of concern, with their things, their circumfusa and the various domains inside which they have traced the limits of their existence - their *nomos*."[49] If we wish to support the narrative self-positioning of individual and collective actors in the geostories of an ‚Anthropocene', we urgently need to expand our stories across the machinic terrain of our existence, scaling our collective agency to govern the ambient commons.

References

Alliez, Eric: Diagrammatic Agency Versus Aesthetic Regime of Contemporary Art: Ernesto Neto's Anti-Leviathan, Deleuze Studies 6.1 (2012), pp. 6-26.

Alliez, Eric: The Cause of the Guattari Effect, trans. Eric Anglès, Shifter Magazine 16 (April 2010), pp. 85-96.

Andreyev, Alex: Introducing data center fabric, the next-generation Facebook data center network, (11/2014), https://code.facebook.com/posts/360346274145943/introducing-data-center-fabric-the-next-generation-facebook-data-center-network/.

Blikstein, Paulo: Digital Fabrication and 'Making' in Education: The Democratization of Invention. In Walter-Herrmann, Julia; Bueching, Corinna (eds.), FabLabs: Of Machines, Makers and Inventors, Berlin: Transcript 2013, pp. 1-21.

46 Latour, Bruno: Agency at the Time of the Anthropocene. 14. The Subcommission on Quaternary Stratigraphy (SQS), a constituent body of the International Commission on Stratigraphy (ICS), has established a Working Group on the Anthropocene: "The 'Anthropocene' is a term widely used since its coining by Paul Crutzen and Eugene Stoermer in 2000 to denote the present time interval, in which many geologically significant conditions and processes are profoundly altered by human activities. These include changes in: erosion and sediment transport associated with a variety of anthropogenic processes, including colonisation, agriculture, urbanisation and global warming; the chemical composition of the atmosphere, oceans and soils, with significant anthropogenic perturbations of the cycles of elements such as carbon, nitrogen, phosphorus and various metals; environmental conditions generated by these perturbations; these include global warming, ocean acidification and spreading oceanic 'dead zones'; the biosphere both on land and in the sea, as a result of habitat loss, predation, species invasions and the physical and chemical changes noted above." http://quaternary.stratigraphy.org/working-groups/anthropocene/. Also see the Anthropocene Project (2013-14), http://www.hkw.de/anthropocene/.

47 Latour. Ibid.

48 Latour. 13.

49 Latour. 14. Emphasis in original.

Bogost, Ian: Procedural Literacy. In: Persuasive Games: The Expressive Power of Videogames. MIT Press 2007, pp. 233-260.

Bowker, Geoffrey C.; Miller, Florence; Ribes, David: Toward Information Infrastructure Studies: Ways of Knowing in a Networked Environment, in Jeremy Hunsinger, Lisbeth Klastrup and Matthew M. Allen (eds), International Handbook of Internet Research, Berlin: Springer Science+Business Media B.V., 2010, pp. 97-117.

Colapinto, John: Material Question, The New Yorker (10/12/2014), http://www.newyorker.com/magazine/2014/12/22/material-question/.

Chui, Michael; Loeffler, Markus; Roberts, Roger: 'The Internet of Things', McKinsey Quarterly (March 2010).http://www.mckinsey.com/insights/high_tech_telecoms_internet/the_internet_of_things/.

De Angelis, Massimo; Harvie, David: The commons. In Martin Parker, George Cheney, Válerie Fournier, Chris Land: The Routledge Companion to Alternative Organization. New York: Routledge 2014, pp. 280-294.

Dragona, Daphne: Counter-Infrastructures: Critical Empowerment and Emancipation in a Networked World. Media-N Journal of the New Media Caucus 10.03 (Fall 2014). http://median.newmediacaucus.org/art-infrastructures-information/counter-infrastructures-critical-empowerment-and-emancipation-in-a-networked-world/.

Essinger, James: Jacquard's Web: How a Hand-Loom Led to the Birth of the Information Age. Oxford: Oxford University Press 2004.

Federici, Silvia: Revolution at Point Zero: Housework, Reproduction, and Feminist Struggle. Oakland, CA: PM Press 2012.

Fonseca, Felipe: Repair Culture. 2015. http://efeefe.no-ip.org/livro/repair-culture/.

Foucault, Michel: The Government of Self and Others: Lectures at the Collège de France, 1982-1983, ed. Arnold I. Davidson, trans. Graham Burchell, New York: Palgrave Macmillan, 2010.

Future Art Base: Power at the End of the Economy: A Discussion with Maurizio Lazzarato, Brian Massumi, Peter Pál Pelbart and Akseli Virtanen, (07/10/2014), http://www.futureartbase.org/2014/10/07/power-at-the-end-of-the-economy-2/.

Genosko, Gary: A-signifying Semiotics, The Public Journal of Semiotics 2.1 (January 2008), pp. 11-21.

Halverson, Erica Rosenfeld; Sheridan, Kimberly M.: The Maker Movement in Education. Harvard Educational Review 84.4 (Winter 2014), pp. 495-504.

Hansen, Mark B. N.: Feed-Forward: On the Future of Twenty-First Century Media. Chicago and London: University of Chicago Press, 2015.

Hayles, Katherine N.: Cognition Everywhere: The Rise of the Cognitive Nonconscious and the Costs of Consciousness, New Literary History 45.2 (Spring 2014), pp. 199-220.

Honey, Margaret; Kanter, David: Design, Make, Play: Growing the Next Generation of STEM Innovators. New York: Routledge 2013.

Hoerl, Erich: A Thousand Ecologies: The Process of Cyberneticization and General Ecology, trans. James Burton, Jeffrey Kirkwood and Maria Vlotides, in Diedrich Diederichsen and Anselm Franke (eds), The Whole Earth: California and the Disappearance of the Outside, Berlin: Sternberg Press, 2013, pp. 121-30.

Kitchin, Rob: Big Data, new epistemologies and paradigm shifts, Big Data & Society 1.1 (April-June 2014), pp. 1-2, http://bds.sagepub.com/content/1/1/2053951714528481.full/.

Lakoff, George; Johnson, Mark: Metaphors We Live By. [1980]. With a new Afterword. Chicago: Chicago University Press 2003.

Lansiti, Marco; Lakhani, Karim T.: 'Digital Ubiquity: How Connections, Sensors, and Data Are Revolutionizing Business', Harvard Business Manager 11 (2014), https://hbr.org/2014/11/digital-ubiquity-how-connections-sensors-and-data-are-revolutionizing-business/.

Latour, Bruno: Agency at the Time of the Anthropocene, New Literary History 45.1 (Winter 2014), pp. 1-18.

Lazzarato, Maurizio: Exiting Language: Semiotic Systems and the Production of Subjectivity in Felix Guattari, transl. Eric Anglés, in: Deborah Hauptmann and Warren Neidich (eds), Cognitive Architecture: From Biopolitics to Noo-politics - Architecture & Mind in the Age of Communication and Information, Rotterdam: 010 Publishers 2010, pp. 502-520.

Lazzarato, Maurizio: Signs and Machines: Capitalism and the Production of Subjectivity, trans. Joshua David Jordan, Los Angeles: Semiotext(e), 2014.

Lem, Stanislaw: Summa Technologiae, trans. Joanna Zylinska, Minneapolis: University of Minnesota Press, 2014.

Linebaugh, Peter: The Magna Carta Manifesto. Liberties and Commons for All. Berkeley, University of California Press 2008.

Linebaugh, Peter: Stop, Thief!: The Commons, Enclosures, and Resistance. Oakland, CA: PM Press 2014.

Lury, Celia; Parisi, Luciana; Terranova, Tiziana: Introduction: The Becoming Topological of Culture, Theory Culture Society 29.4-5 (2012), pp. 3-35.

Manovich, Lev: Software is the Message. Journal of Visual Culture 13.1 (April 2014), pp. 79-81.

Manovich, Lev: The Language of New Media. Cambridge, MA: MIT Press 2001.

McCullough, Malcolm: Ambient Commons: Attention in the Age of Embodied Information. Cambridge, MA: MIT Press 2013.

McCullough, Malcolm: Governing the Ambient Commons. Hedgehog Review. 16.2 (Summer), pp. 44-55.

Open Network Foundation: Software-Defined Networking: The New Norm for Networks, ONF White Paper (04/12/2012), https://www.opennetworking.org/images/stories/downloads/sdn-resources/white-papers/wp-sdn-newnorm.pdf/.

Ostrom, Elinor. Governing the commons: the evolution of institutions for collective action. Cambridge New York: Cambridge University Press 1990.

Ostrom, Elinor; Hess, Charlotte. Understanding Knowledge as a Commons: from theory to practice. Cambridge, Massachusetts: MIT Press 2011.

Raunig, Gerald: A Thousand Machines: A Concise Philosophy of the Machine as Social Movement, trans. Aileen Derieg. New York: Semiotext(e) 2010.

Sharples, Mike; Adams, Anne; Ferguson, Rebecca; Gaved, Mark; McAndrew, Patrick;, Rienties, Bart; Weller, Martin; Whitelock, Denise: Innovating Pedagogy: Open University Innovation Report 3. Milton Keynes: The Open University 2014.

Shepard, Mark: Toward the Sentient City, in Mark Shepard (ed): Sentient City: Ubiquitous Computing, Architecture, and the Future of Urban Space, Cambridge, MA: MIT Press 2011, pp. 15-26.

Schoen, Sandra; Ebner, Martin; Kumar, Swapna: The Maker Movement. Implications of new digital gadgets, fabrication tools and spaces for creative learning and teaching. eLearning Papers. Open Education Europa 2014. http://www.openeducationeuropa.eu/de/article/The-Maker-Movement.-Implications-of-new-digital-gadgets,-fabrication-tools-and-spaces-for-creative-learning-and-teaching/.

Streeck, Juergen; Goodwin, Charles; LeBaron, Curtis (eds): Embodied Interaction: Language and Body in the Material World. Cambridge University Press 2014.

Wiedemann, Carolin; Zehle, Soenke (eds): Depletion Design: A Glossary of Network Ecologies. Theory on Demand #8. Amsterdam: Institute of Network Cultures, 2012.

Yakowitz, Jane: Tragedy of the Data Commons. Harvard Journal of Law & Technology. 25.1 (Fall 2011), pp. 1-67.

Zehle, Soenke. 'Documenting Depletion: Of Algorithmic Machines, Experience Streams, and Plastic People '. In: Richard Maxwell, Jon Raundalen, and Nina Lager Vesterberg (eds), Media and the Ecological Crisis, London: Routledge 2015, pp. 52-68.

Zuiderwijk, Anneke; Janssen, Marijn; Davis, Chris: Innovation with open data: Essential elements of open data ecosystems. Information Polity: The International Journal of Government & Democracy in the Information Age 19.1-2 (2014), pp. 17-33.

Zylinska, Joanna: Minimal Ethics for the Anthropocene, Ann Arbor: Open Humanities Press 2014.

Roba Abbas, Katina Michael, M.G. Michael:

Using a Social-Ethical Framework to Evaluate Location-Based Services in an Internet of Things World

Abstract:

The idea for an Internet of Things has matured since its inception as a concept in 1999. People today speak openly of a Web of Things and People, and even more broadly of an Internet of Everything. As our relationships become more and more complex and enmeshed, through the use of advanced technologies, we have pondered on ways to simplify flows of communications, to collect meaningful data, and use them to make timely decisions with respect to optimisation and efficiency. At their core, these flows of communications are pathways to registers of interaction, and tell the intricate story of outputs at various units of analysis- things, vehicles, animals, people, organisations, industries, even governments. In this trend toward evidence-based enquiry, data is the enabling force driving the growth of IoT infrastructure. This paper uses the case of location-based services, which are integral to IoT approaches, to demonstrate that new technologies are complex in their effects on society. Fundamental to IoT is the spatial element, and through this capability, the tracking and monitoring of everything, from the smallest nut and bolt, to the largest shipping liner to the mapping of planet earth, and from the whereabouts of the minor to that of the prime minister. How this information is stored, who has access, and what they will do with it, is arguable depending on the stated answers. In this case study of location-based services we concentrate on control and trust, two overarching themes that have been very much neglected, and use the outcomes of this research to inform the development of a socio-ethical conceptual framework that can be applied to minimise the unintended negative consequences of advanced technologies. We posit it is not enough to claim objectivity through information ethics approaches alone, and present instead a socio-ethical impact framework. Sociality therefore binds together that higher ideal of praxis where the living thing (e.g. human) is the central and most valued actor of a system.

Agenda:

ISSN 1614-1687

Authors:

Honorary Fellow Dr Roba Abbas:

- School of Information Systems and Technology, University of Wollongong, Northfields Avenue, Wollongong NSW 2522, Australia
- ☎ + 612 - 4221 - 3555 , ✉ roba@uow.edu.au 💻http://www.technologyandsociety.org/members/2013/7/25/dr-roba-abbas
- Relevant publications:
  - *R. Abbas, K. Michael, M.G. Michael, R. Nicholls, Sketching and validating the location-based services (LBS) regulatory framework in Australia, Computer Law and Security Review 29, No.5 (2013): 576-589.*
  - *R. Abbas, K. Michael, M.G. Michael, The Regulatory Considerations and Ethical Dilemmas of Location-Based Services (LBS): A Literature Review, Information Technology & People 27, No.1 (2014): 2-20.*

Associate Professor Katina Michael:

- School of Information Systems and Technology, University of Wollongong, Northfields Avenue, Wollongong NSW 2522, Australia
- ☎ + 612 - 4221 - 3937 , ✉ katina@uow.edu.au 💻 http://ro.uow.edu.au/kmichael
- Relevant publications:
  - *K. Michael, R. Clarke, Location and Tracking of Mobile Devices: Überveillance Stalks the Streets, Computer Law and Security Review 29, No.3 (2013): 216-228.*
  - *K. Michael, M. G. Michael, Innovative Automatic Identification and Location-Based Services: From Bar Codes to Chip Implants, IGI Global, (2009).*
  - *L. Perusco, K. Michael, Control, trust, privacy, and security: evaluating location-based services, IEEE Technology and Society Magazine 26, No.1 (2007): 4-16.*

Honorary Associate Professor M.G. Michael

- School of Information Systems and Technology, University of Wollongong, Northfields Avenue, Wollongong NSW 2522, Australia
- ☎ + 612 – 4221 - 3937, ✉ mgm@uow.edu.au, 💻 http://ro.uow.edu.au/mgmichael
- Relevant publications:
  - *M.G. Michael and K. Michael (eds) Uberveillance and the Social Implications of Microchip Implants: Emerging Technologies, Hershey: PA, IGI Global, (2013).*
  - *K. Michael, M. G. Michael, "The Social and Behavioral Implications of Location-Based Services, Journal of Location-Based Services, Volume 5, Issue 3-4, (2011), 121-137.*
  - *M.G. Michael, K. Michael, Towards a State of Uberveillance, IEEE Technology and Society Magazine, 29, No.2, (2010): 9-16.*
  - *M. G. Michael, S. J. Fusco, K. Michael, A Research Note on Ethics in the Emerging Age of Uberveillance, Computer Communications, 31 No.6, 2008: 1192-1199.*

Introduction

Locative technologies are a key component of the Internet of Things (IoT). Some scholars go so far as to say it is the single most important component that enables the monitoring and tracking of subjects and objects. Knowing where something or someone is, is of greater importance than knowing who they are because *it* or *they* can be found, independent of *what* or *who* they are. Location also grants us that unique position on the earth's surface, providing for us one of the vital pieces of information forming the distance, speed, time matrix. A unique ID, formed around an IP address in an IoT world, presents us with the capability to label every living and non-living thing and to recollect it, adding to its history and longer term physical lifetime. But without knowing where something is, even if we have the knowledge that an action is required toward some level of maintenance, we cannot be responsive. Since the introduction of electronic databases, providing accurate records for transaction processing has been a primary aim. Today, however, we are attempting to increase visibility using high resolution geographic details, we are contextualizing events through discrete and sometimes continuous sensor-based rich audio-visual data collection, and we are observing how mobile subjects and objects interact with the built environment. We are no longer satisfied with an approach that says *identify all things*, but we wish to be able to recollect or activate them on demand, understand associations and affiliations, creating a digital chronicle of its history to provide insights toward sustainability.

There is thus an undue pressure on the ethical justification for social and behavioral tracking of people and things in everyday life. Solely because we have the means to do something, it does not mean we should do it. We are told that through this new knowledge gained from big data we can reduce carbon emissions, we can eradicate poverty, we can grant all people equity in health services, we can better provision for expected food shortages, utilize energy resources optimally, in short, make the world a better place. This utopian view might well be the vision that the tech sector wish to adopt as an honourable marketing strategy, but the reality of thousands of years of history tells us that technology does not necessarily on its own accord, make things better. In fact, it has often made some aspects of life, such as conflict and war, much worse through the use of modern, sophisticated advanced techniques. We could argue that IoT will allow for care-based surveillance that will bring about aid to individuals and families given needs, but the reality is that wherever people are concerned, technology may be exploited towards a means for control. Control on its own is not necessarily an evil, it all depends on how the functionality of given technologies are applied. Applied negatively the recipient of this control orientation learns distrust instead of trust which then causes a chain reaction throughout society, especially with respect to privacy and security. We need only look at the techniques espoused by some governments in the last 200 years to acknowledge that heinous crimes against humanity (e.g. democide) have been committed with new technological armaments (Rummel, 1997) to the detriment of the citizenry.

A socio-ethical framework is proposed as a starting point for seeking to understand the social implications of location services, applicable to current and future applications within IoT infrastructure. To stop at critiquing services using solely an information ethics-based approach is to fall short. Today's converging services and systems require a greater scope of orientation to ask more generally how society may be affected at large, not just whether information is being collected, stored, and shared appropriately. To ask questions about how location services and IoT technology will directly and indirectly change society has far greater importance for the longer term vision of person-to-person and person-to-thing interactions than simply studying various attributes in a given register.

Studies addressing the social implications of emerging technologies, such as LBS, generally reflect on the risks and ethical dilemmas resulting from the implementation of a particular technology within a given social context. While numerous approaches to ethics exist, all are inextricably linked to ideas of morality, and an ability to distinguish good conduct from bad. Ethics, in simple terms, can be considered as the "study of morality" (Quinn 2006, p. 55), where morality refers to a "system of rules for guiding human conduct and principles for evaluating those rules" (Tavani 2007, p. 32). This definition is shared by Elliot and Phillips (2004, p. 465), who regard ethics as "a set of rules, or a decision procedure, or both, intended to provide the conditions under which the greatest number of human beings can succeed in 'flourishing', where 'flourishing' is defined as living a fully human life" (O'Connor and Godar 2003, p. 248).

According to the literature, there are two prominent ethical dilemmas that emerge with respect to locating a person or thing in an Internet of Things world. First, the risk of unauthorised disclosure of one's location which is a breach of privacy; and second the possibility of increased monitoring leading to unwarranted surveillance by institutions and individuals. The socio-ethical implications of LBS in the context of IoT can therefore be explored based on these two major factors. IoT more broadly, however, can be examined by studying numerous social and ethical dilemmas from differing perspectives. Michael et al. (2006a, pp. 1-10) propose a framework for considering the ethical challenges emerging from the use of GPS tracking and monitoring solutions in the control, convenience and care usability contexts. The authors examine these contexts in view of the four ethical dimensions of privacy, accuracy, property and accessibility (Michael et al. 2006a, pp. 4-5). Alternatively, Elliot and Phillips (2004, p. 463) discuss the social and ethical issues associated with m-commerce and wireless computing in view of the privacy and access, security and reliability challenges. The authors claim that factors such as trust and control are of great importance in the organisational context (Elliot and Phillips 2004, p. 470). Similar studies propose that the major themes regarding the social implications of LBS be summarised as control, trust, privacy and security (Perusco et al. 2006; Perusco and Michael 2007). These themes provide a conceptual framework for reviewing relevant literature in a structured fashion, given that a large number of studies are available in the respective areas.

This article, in the first instance, focusses on the control- and trust-related socio-ethical challenges arising from the deployment of LBS in the context of IoT, two themes that are yet to receive comprehensive coverage in the literature. This is followed by an examination of LBS in the context of the Internet of Things (IoT), and the ensuing ethical considerations. A socio-ethical framework is proposed as a valid starting point for addressing the social implications of LBS and delivering a conceptual framework that is applicable to current LBS use cases and future applications within an Internet of Things world.

Control

Control, according to the Oxford Dictionary (2012a), refers to the "the power to influence or direct people's behaviour or the course of events". With respect to LBS, this theme is examined in terms of a number of important concepts, notably surveillance, dataveillance, sousveillance and überveillance scholarship.

Surveillance

A prevailing notion in relation to control and LBS is the idea of exerting power over individuals through various forms of surveillance. Surveillance, according to sociologist David Lyon, "is the focused, systematic and routine attention to personal details for the purposes of influence, management, protection and or direction," although Lyon admits that there are exceptions to this general definition (Lyon 2007, p. 14). Surveillance has also been described as the process of methodically monitoring the behaviour, statements, associates, actions and/or communications of an individual or individuals, and is centred on information collection (Clarke 1997; Clarke 2005, p. 9).

The act of surveillance, according to Clarke (1988; 1997) can either take the form of personal surveillance of a specific individual or mass surveillance of groups of interest. Wigan and Clarke (2006, p. 392) also introduce the categories of object surveillance of a particular item and area surveillance of a physical enclosure. Additional means of expressing the characteristics of surveillance exist. For example, the phrase "surveillance schemes" has been used to describe the various surveillance initiatives available (Clarke 2007a, p. 28). Such schemes have been demonstrated through the use of a number of mini cases or vignettes, which include, but are not limited to, baby monitoring, acute health care, staff movement monitoring, vehicle monitoring, goods monitoring, freight interchange-point monitoring, monitoring of human-attached chips, monitoring of human-embedded chips, and continuous monitoring of chips (Clarke 2007c; Clarke 2007b, pp. 47-60). The vignettes are intended to aid in understanding the desirable and undesirable social impacts resulting from respective schemes.

Common surveillance metaphors

In examining the theme of control with respect to LBS, it is valuable to initially refer to general surveillance scholarship to aid in understanding the link between LBS and surveillance. Surveillance literature is somewhat dominated by the use of metaphors to express the phenomenon. A prevalent metaphor is that of the panopticon, first introduced by Jeremy Bentham (Bentham and Bowring 1843), and later examined by Michel Foucault (1977). Foucault's seminal piece *Discipline and Punish* traces the history of punishment, commencing with the torture of the body in the eighteenth century, through to more modern forms of punishment targeted at the soul (Foucault 1977). In particular, Foucault's account offers commentary on the notions of surveillance, control and power through his examination of Bentham's panopticon, which are pertinent in analysing surveillance in general and monitoring facilitated by LBS in particular. The panopticon, or "Inspection-House" (Bentham and Bowring 1843, p. 37), refers to Bentham's design for a prison based on the essential notion of "seeing without being seen" (p. 44). The architecture of the panopticon is as follows:

> *"The building is circular. The apartments of the prisoners occupy the circumference. You may call them, if you please, the cells... The apartment of the inspector occupies the centre; you may call it if you please the inspector's lodge. It will be convenient in most, if not in all cases, to have a vacant space or area all round, between such centre and such circumference. You may call it if you please the intermediate or annular area"* (Bentham and Bowring 1843, pp. 40-41).

Foucault (1977, p. 200) further illustrates the main features of the inspection-house, and their subsequent implications on constant visibility:

> *"By the effect of backlighting, one can observe from the tower ['lodge'], standing out precisely against the light, the small captive shadows in the cells of the periphery. They are like so many cages, so many small theatres, in which each actor is alone, perfectly individualized and constantly visible...Full lighting and the eye of a supervisor ['inspector'] capture better than darkness, which ultimately protected. Visibility is a trap."*

While commonly conceived as ideal for the prison arrangement, the panopticon design is applicable and adaptable to a wide range of establishments, including but not limited to work sites, hospital, schools, and/or or any establishment in which individuals "are to be kept under inspection" (Bentham and Bowring 1843, p. 37). It has been suggested, however, that the panopticon functions as a tool for mass (as opposed to personal) surveillance in which large numbers of individuals are monitored, in an efficient sense, by a small number (Clarke 2005, p. 9). This differs from the more efficient, automated means of dataveillance (to be shortly examined). In enabling mass surveillance, the panopticon theoretically allows power to be. In examining the theme of control with respect to LBS, it is valuable to initially refer to general surveillance scholarship to aid in understanding the link between LBS and surveillance. Surveillance literature is somewhat dominated by the use of metaphors to express the phenomenon. Foucault (1977, pp. 202-203) provides a succinct summary of this point:

> *"He who is subjected to a field of visibility, and who knows it, assumes responsibility for the constraints of power; he makes them play spontaneously upon himself; he inscribes in himself the power relation in which he simultaneously plays both roles; he becomes the principle of his own subjection."*

This self-disciplinary mechanism functions similarly, and can somewhat be paralleled, to various notions in George Orwell's classic novel *Nineteen Eighty Four* (Orwell 1949), also a common reference point in surveillance literature. *Nineteen Eighty Four* has been particularly influential in the surveillance realm, notably due to the use of "Big Brother" as a symbol of totalitarian, state-based surveillance. Big Brother's inescapable presence is reflected in the nature of surveillance activities. That is, that monitoring is constant and omnipresent and that "[n]othing was your own except the few cubic centimetres inside your skull" (Orwell 1949, p. 29). The oppressive authority figure of Big Brother possesses the ability to persistently monitor and control the lives of individuals, employing numerous mechanisms to exert power and control over his populace as a reminder of his unavoidable gaze.

One such mechanism is the use of telescreens as the technological solution enabling surveillance practices to be applied. The telescreens operate as a form of self-disciplinary tool by way of reinforcing the idea that citizens are under constant scrutiny (in a similar fashion to the inspector's lodge in the panopticon metaphor). The telescreens inevitably influence behaviours, enabling the state to maintain control over actions and thoughts, and to impose appropriate punishments in the case of an offence. This is demonstrated in the following excerpt:

> "It was terribly dangerous to let your thoughts wander when you were in any public place or within range of a telescreen. The smallest thing could give you away. A nervous tic, an unconscious look of anxiety, a habit of muttering to yourself – anything that carried with it the suggestion of abnormality, of having something to hide. In any case, to wear an improper expression on your face (to look incredulous when a victory was announced, for example) was itself a punishable offence" (Orwell 1949, p. 65).

The Internet of Things, with its ability to locate and determine *who* is or *what* is related to one another using a multiplicity of technologies, will enable authorities in power to infer what someone is likely to do in a given context. Past behavioural patterns, can for example, reveal a likely course of action with relatively no prediction required. IoT in all its glory will provide complete visibility- the question is what are the risks associated with providing that kind of capability to the state or private enterprise? In scenario analysis we can ponder how IoT in a given context will be used for good, how it will be used for bad, and a neutral case where it will have no effect whatsoever because the data stream will be ignored by the system owner. While IoT has been touted as the ultimate in providing great organisational operational returns, one can see how it can lend itself to location-based tracking and monitoring using a panopticon metaphor. Paper records and registers were used during World War 2 for the purposes of segregation, IoT and especially the ability to "locate on demand", may well be used for similar types of control purposes.

Applying surveillance metaphors to LBS

The aforementioned surveillance metaphors can be directly applied to the case of LBS within IoT. In the first instance, it can be perceived that the exploitation of emerging technologies, such as LBS, extends the notion of the panopticon in a manner that allows for inspection or surveillance to take place regardless of geographic boundaries or physical locations. When applying the idea of the panopticon to modern technologies, Lyon suggests that "Bentham's panopticon gives way to the electronic superpanopticon" (Lyon 2001, p. 108). With respect to LBS, this superpanopticon is not limited to and by the physical boundaries of a particular establishment, but is rather reliant on the nature and capabilities of the mobile devices used for 'inspection'. In an article titled "The Panopticon's Changing Geography", Dobson and Fischer (2007) also discuss progress and various manifestations of surveillance technology, specifically the panopticon, and the consequent implications on power relationships. From Bentham's architectural design, to the electronic panopticon depicted by Orwell, and contemporary forms of electronic surveillance including LBS and covert human tracking, Dobson and Fisher (2007, p. 308-311) claim that all forms of watching enable continuous surveillance either as part of their primary or secondary purpose. They compare four means of surveillance- analogue technologies as used by spies which have unlimited geographic coverage and are very expensive to own and operate, Bentham's original panopticon where the geographic view was internal to a building, George Orwell's big brother view which was bound by the extent of television cables, and finally human tracking systems which were limited only by the availability and granularity of cell phone towers.

A key factor in applying the panopticon metaphor to IoT is that individuals, through the use of mobile location devices and technologies, will be constantly aware of their visibility and will assume the knowledge that an 'inspector' may be monitoring their location and other available information remotely at any given time. Mobile location devices may similarly replace Orwell's idea of the telescreens as Big Brother's primary surveillance technology, resulting in a situation in which the user is aiding in the process of location data collection and thereby surveillance. This creates, as maintained by Andrejevic (2007, p. 95), a "widening 'digital enclosure' within which a variety of interactive devices that provide convenience and customization to users double as technologies for gathering information about them."

'Geoslavery'

Furthermore, in extreme situations, LBS may facilitate a new form of slavery, "geoslavery", which Dobson and Fischer (2003, pp. 47-48) reveal is "a practice in which one entity, the master, coercively or surreptitiously monitors and exerts control over the physical location of another individual, the slave. Inherent in this concept is the potential for a master to routinely control time, location, speed, and direction for each and every movement of the slave or, indeed, of many slaves simultaneously." In their seminal work, the authors flag geoslavery as a fundamental human rights issue (Dobson and Fisher 2003, p. 49), one that has the potential to somewhat fulfil Orwell's Big Brother prophecy, differing only in relation to the sophistication of LBS in comparison to visual surveillance and also in terms of who is in control. While Orwell's focus is on the state, Dobson and Fischer (2003, p. 51) caution that geoslavery can also be performed by individuals "to control other individuals or groups of individuals."

From state-based to citizen level surveillance

Common in both *Discipline and Punish* and *Nineteen Eighty Four* is the perspective that surveillance activities are conducted at the higher level of the "establishment"; that is, institutional and/or state-based surveillance. However, it must be noted that similar notions can be applied at the consumer or citizen level. Mark Andrejevic (2007, p. 212), in his book *iSpy: Surveillance and Power in the Interactive Era*, terms this form of surveillance as "lateral or peer-to-peer surveillance." This form of surveillance is characterised by "increasing public access to the means of surveillance – not just by corporations and the state, but by individuals" (Andrejevic 2007, p. 212). Similarly, Barreras and Mathur (2007, pp. 176-177) state that wireless location tracking capabilities are no longer limited to law enforcement, but are open to any interested individual. Abbas et al. (2011, pp. 20-31) further the discussion by focussing on related notions, explicitly, the implications of covert LBS-based surveillance at the community level, where technologies typically associated with policing and law enforcement are increasingly available for use by members of the community. With further reference to LBS, Dobson and Fischer (2003, p. 51) claim that the technology empowers individuals to control other individuals or groups, while also facilitating extreme activities. For instance, child protection, partner tracking and employee monitoring can now take on extreme forms through the employment of LBS (Dobson and Fisher 2003, p. 49). According to Andrejevic (2007, p. 218), this "do-it-yourself" approach assigns the act of monitoring to citizens. In essence higher degrees of control are granted to individuals thereby encouraging their participation in the surveillance process (Andrejevic 2007, pp. 218-222). It is important to understand IoT in the context of this multifaceted "watching". IoT will not only be used by organisations and government agencies, but individuals in a community will also be granted access to information at small units of aggregated data. This has implications at a multiplicity of levels. Forces of control will be manifold.

Dataveillance

The same sentiments can be applied to the related, and to an extent superseding, notion of data surveillance, commonly referred to as *dataveillance*. Coined by Roger Clarke in the mid-eighties, dataveillance is defined as "the systematic use of personal data systems in the investigation or monitoring of the actions or communications of one or more persons" (Clarke 1988). Clarke (2005, p. 9) maintains that this process is automated and therefore a relatively economical activity when compared with other forms of surveillance, in that dataveillance activities are centred on examination of the data trails of individuals. For example, traditional forms of surveillance rely on expensive visual monitoring techniques, whereas dataveillance is largely an economically efficient alternative (Clarke 1994; 2001d, p. 11). Visual behavioural monitoring (that is, traditional surveillance) is an issue, but is nonetheless overshadowed by the challenges associated with dataveillance, particularly with reference to personal and mass dataveillance (Clarke 2005, pp. 9-10). That is, *personal dataveillance* presents risks to the individual based primarily on the potential for the collected data/information to be incorrect or outdated, while *mass dataveillance* is risky in that it may generate suspicion amongst individuals (Albrecht & Michael, 2013).

Risks associated with dataveillance

Clarke's early and influential work on "Information Technology and Dataveillance" recognises that information technology is accelerating the growth of dataveillance, which presents numerous benefits and risks (Clarke 1988, pp. 498, 505-507). Clarke lists advantages in terms of safety and government applications, while noting the dangers associated with both personal and mass dataveillance (Clarke 1988, pp. 505-507). These risks can indeed be extended or applied to the use of location and tracking technologies to perform dataveillance activities, resulting in what can be referred to as "dataveillance on the move" (Michael and Michael 2012). The specific risks include: ability for behavioural patterns to be exposed and cross-matched, potentially for revelations that may be harmful from a political and personal perspective, rise in the use of "circumstantial evidence", transparency of behaviour resulting in the misuse of information relating to an individual's conduct, and "actual repression of the readily locatable and trackable individual" (Clarke 2001b, p. 219). Emerging from this analysis, and that concerning surveillance and related metaphors, is the significant matter of loss of control.

Loss of control

Michael et al. (2006a, p. 2) state, in the context of GPS tracking, that the issue of control is a leading ethical challenge given the invasive nature of this form of monitoring. The mode of control can differ depending on the context. For instance, the business context may include control through directing or 'pushing' advertisements to a specific individual, and at personal/individual level could signify control in the manner of "self-direction" (Perusco et al. 2006, p. 93). Other forms of social control can also be exercised by governments and organisations (Clarke 2003b), while emerging LBS solutions intended for the consumer sector extend the notion of control to community members (Abbas et al. 2011). This is an area that has not been adequately addressed in the literature. The subsequent risks to the individual are summarised in the following passage:

> *"Location technologies therefore provide, to parties that have access to the data, the power to make decisions about the entity subject to the surveillance, and hence exercise control over it. Where the entity is a person, it enables those parties to make determinations, and to take action, for or against that person's interests. These determinations and actions may be based on place(s) where the person is, or place(s) where the person has been, but also on place(s) where the person is not, or has not been"* (Wigan and Clarke 2006, p. 393).

Therefore GPS and other location devices and technologies may result in decreased levels of control from the perspective of the individual being monitored. For example, in an article based on the use of scenarios to represent the social implications associated with the implementation of LBS, Perusco and Michael (2007) demonstrate the various facets of control in relation to LBS. The discussion is generally centred on the loss of control which can be experienced in numerous ways, such as when a device does not accurately operate, or when an individual constantly monitors a family member in an attempt to care for them (Perusco and Michael 2007, pp. 6-7, 10). The authors raise valuable ideas with respect to control, such as the need to understand the purpose of control, the notion of consent, and developing methods to deal with location inaccuracies amongst others (p. 14). Perusco and Michael further assert that control has a flow-on effect on other issues, such as trust for instance, with the authors questioning whether it is viable to control individuals given the likely risk that trust may be relinquished in the process (p. 13).

Concurrent with loss of control, the issue of pre-emptive control with respect to LBS is a delicate one, specifically in relation to suspected criminals or offenders. Perusco et al. (2006, p. 92) state that the punishment of a crime is typically proportionate to the committed offence, thus the notion of pre-emptive monitoring can be considered fundamentally flawed given that individuals are being punished without having committed an offence. Rather, they are suspected of being a threat. According to Clarke and Wigan (2011), a person is perceived a threat, based on their "personal associations" which can be determined using location and tracking technologies to establish the individual's location in relation to others, and thus control them based on such details. This is where IoT fundamentally comes into play. While location information can tell us much about where an individual is at any point in time, it is IoT that will reveal the inter-relationships and frequency of interaction, and specific application of measurable transactions. IoT is that layer that will bring things to be scrutinized in new ways.

This calls for an evaluation of LBS solutions that can be used for covert operations. Covert monitoring using LBS is often considered a useful technique, one that promotes less opposition than overt forms of monitoring, as summarised below:

> *"Powerful economic and political interests are seeking to employ location and tracking technologies surreptitiously, to some degree because their effectiveness is greater that way, but mostly in order to pre-empt opposition"* (Clarke 2001b, p. 221).

Covert applications of LBS are increasingly available for the monitoring and tracking of social relations such as a partner or a child (Abbas et al. 2011). Regardless of whether covert or overt, using LBS for monitoring is essentially about control, irrespective of whether the act of controlling is motivated by necessity, or for more practical or supportive purposes (Perusco et al. 2006, p. 93).

Studies focussing on user requirements for control

The control dimension is also significant in studies focussing on LBS users, namely, literature concerned with user-centric design, and user adoption and acceptance of LBS and related mobile solutions. In a paper focussing on understanding user requirements for the development of LBS, Bauer et al. (2005, p. 216) report on a user's "fear" of losing control while interacting with mobile applications and LBS that may infringe on their personal life. The authors perceive loss of control to be a security concern requiring attention, and suggest that developers attempt to relieve the apprehension associated with increased levels of personalisation though ensuring that adequate levels of control are retained (Bauer et al. 2005, p. 216). This is somewhat supported by the research of Xu and Teo (2004, pp. 793-803), in which the authors suggest that there exists a relationship between control, privacy and intention to use LBS. That is, a loss of control results in a privacy breach, which in turn impacts on a user's intention to embrace LBS.

The aforementioned studies, however, fail to explicitly incorporate the concept of value into their analyses. Due to the lack of literature discussing the three themes of privacy, value and control, Renegar et al. (2008, pp. 1-2) present the privacy-value-control (PVC) trichotomy as a paradigm beneficial for measuring user acceptance and adoption of mobile technologies. This paradigm stipulates the need to achieve harmony amongst the concepts of privacy, value and control in order for a technology to be adopted and accepted by the consumer. However, the authors note that perceptions of privacy, value and control are dependent on a number of factors or entities, including the individual, the technology and the service provider (Renegar et al. 2008, p. 9). Consequently, the outcomes of Renegar et al.'s study state that privacy does not obstruct the process of adoption but rather the latter must take into account the value proposition in addition to the amount of control granted.

Monitoring using LBS: control versus care?

The focus of the preceding sections has been on the loss of control, the dangers of pre-emptive control, covert monitoring, and user perspectives relating to the control dimension. However, this analysis should not be restricted to the negative implications arising from the use of LBS, but rather should incorporate both the control and care applications of LBS. For instance, while discussions of surveillance and the term in general typically invoke sinister images, numerous authors warn against assuming this subjective viewpoint. Surveillance should not be considered in itself as disagreeable. Rather, "[t]he problem has been the presumptiveness of its proponents, the lack of rational evaluation, and the exaggerations and excesses that have been permitted" (Clarke 2007a, p. 42). This viewpoint is reinforced in the work of Elliot and Phillips (2004, p. 474), and can also be applied to dataveillance.

The perspective that surveillance inevitability results in negative consequences such as individuals possessing excessive amounts of control over each other should be avoided. For instance, Lyon (2001, p. 2) speaks of the dual aspects of surveillance in that "[t]he same process, surveillance – watching over – both enables and constrains, involves care and control." Michael et al. (2006a) reinforce such ideas in the context of GPS tracking

and monitoring. The authors claim that GPS tracking has been employed for control purposes in various situations, such as policing/law enforcement, the monitoring of parolees and sex offenders, the tracking of suspected terrorists and the monitoring of employees (Michael et al. 2006a, pp. 2-3). However, the authors argue that additional contexts such as convenience and care must not be ignored, as GPS solutions may potentially simplify or enable daily tasks (convenience) or be used for healthcare or protection of vulnerable groups (care) (Michael et al. 2006a, pp. 3-4). Perusco and Michael (2005) further note that the tracking of such vulnerable groups indicates that monitoring activities are no longer limited to those convicted of a particular offence, but rather can be employed for protection and safety purposes. Table 1 provides a summary of GPS tracking and monitoring applications in the control, convenience and care contexts, adapted from Michael et al. (2006a, pp. 2-4), identifying the potentially constructive uses of GPS tracking and monitoring.

Table 1: GPS monitoring applications in the control, convenience and care contexts, adapted from Michael et al. (2006a, pp. 2-4)

Context	Applications
Control	Law enforcement Parolees and sex offenders tracking Suspected terrorists tracking Employee monitoring
Convenience	Vehicle tracking Child/family member/friend tracking Sport-related applications
Care	Monitoring of dementia sufferers Child tracking

It is crucial that in evaluating LBS control literature and establishing the need for LBS regulation, both the control and care perspectives are incorporated. The act of monitoring should not immediately conjure up sinister thoughts. The focus should preferably be directed to the important question of purpose or motives. Lyon (2007, p. 3) feels that purpose may exist anywhere on the broad spectrum between care and control. Therefore, as expressed by Elliot and Phillips (2004, p. 474), a crucial factor in evaluating the merit of surveillance activities and systems is determining "how they are used." These sentiments are also applicable to dataveillance. It is helpful at this point to discuss alternative and related practices that may incorporate location information throughout the monitoring process.

Sousveillance

The term sousveillance, coined by Steve Mann, comes from the French terms *sous* which means *from below*, and veiller which means *to watch* (Mann et al. 2003, p. 332). It is primarily a form of "inverse surveillance" (Mann et al. 2003, p. 331), whereby an individual is in essence "surveilling the surveillers" (p. 332). Sousveillance is reliant on the use of wearable computing devices to capture *audiovisual* and *sensory* data (Mann 2005, p. 625). A major concern with respect to sousveillance, according to Mann (2005, p. 637), is the dissemination of the recorded data which for the purposes of this investigation, may include images of locations and corresponding geographic coordinates.

Sousveillance, 'reflectionism' and control

Relevant to the theme of control, it has been argued that sousveillance can be utilised as a form of resistance to unwarranted surveillance and control by institutions. According to Mann et al. (2003, p. 333), sousveillance is a type of reflectionism in which individuals can actively respond to bureaucratic monitoring and to an extent

"neutralize surveillance". Sousveillance can thus be employed in response to social control in that surveillance activities are reversed:

> *"The surveilled become sousveillers who engage social controllers (customs officials, shopkeepers, customer service personnel, security guards, etc.) by using devices that mirror those used by these social controllers"* (Mann et al. 2003, p. 337).

Sousveillance differs from surveillance in that traditional surveillance activities are "centralised" and "localized." It is dispersed in nature and "delocalized" in its global coverage (Ganascia 2010, p. 496). As such, sousveillance requires new metaphors for understanding its fundamental aspects. A useful metaphor proposed by Ganascia (2010, p. 496) for describing sousveillance is the canopticon, which can be contrasted to the panopticon metaphor. At the heart of the canopticon are the following principles:

> *"total transparency of society, fundamental equality, which gives everybody the ability to watch – and consequently to control – everybody else, [and] total communication, which enables everyone to exchange with everyone else"* (Ganascia 2010, p. 497).

This exchange may include the dissemination of location details, thus signalling the need to incorporate sousveillance into LBS regulatory discussions. A noteworthy element of sousveillance is that it shifts the ability to control from the state/institution (surveillance) to the individual. While this can initially be perceived as an empowering feature, excessive amounts of control, if unchecked, may prove detrimental. That is, control may be granted to individuals to disseminate their location (and other) information, or the information of others, without the necessary precautions in place and in an unguarded fashion. The implications of this exercise are sinister in their extreme forms. When considered within the context of IoT, sousveillance ideals are likely compromised. Yes, I can fight back against state control and big brother with sousveillance but in doing so I unleash potentially a thousand or more little brothers, each with their capacity to (mis)use the information being gathered.

Towards überveillance

The concepts of surveillance, dataveillance and sousveillance have been examined with respect to their association with location services in an IoT world. It is therefore valuable, at this point, to introduce the related notion of überveillance. Überveillance, a term coined by M.G. Michael in 2006, can be described as "an omnipresent electronic surveillance facilitated by technology that makes it possible to embed surveillance devices in the human body" (Michael et al. 2006b; Macquarie Dictionary 2009, p. 1094). Überveillance combines the dimensions of identification, location and time, potentially allowing for forecasting and uninterrupted real-time monitoring (Michael and Michael 2007, pp. 9-10), and in its extreme forms can be regarded as "Big Brother on the inside looking out" (p. 10).

Überveillance is considered by several authors to be the contemporary notion that will supplant surveillance. For instance, Clarke (2007a, p. 27) suggests that the concept of surveillance is somewhat outdated and that contemporary discussions be focussed on the notion of überveillance. It has further been suggested that überveillance is built on the existing notion of dataveillance. That is, "[ü]berveillance takes that which was static or discrete in the dataveillance world, and makes it constant and embedded" (Michael and Michael 2007, p. 10). The move towards überveillance thus marks the evolution from physical, visual forms of monitoring (surveillance), through to the increasingly sophisticated and ubiquitous embedded chips (überveillance) (Michael & Michael 2010; Gagnon et al. 2013). Albrecht and McIntyre (2005) describe these embedded chips as "spychips" and were focused predominantly on RFID tracking of people through retail goods and services. They spend considerable space describing the Internet of Things concept. Perakslis and Wolk (2006) studied the social acceptance of RFID implants as a security method and Perakslis later went on to incorporate überveillance into her research into behavioural motivators and personality factors toward adoption of humancentric IoT applications.

Given that überveillance is an emerging term (Michael and Michael 2007, p. 9), diverse interpretations have been proposed. For example, Clarke (2007a) offers varying definitions of the term, suggesting that überveillance can be understood as any of the following: *omni-surveillance*, an apocalyptic notion that "applies across all space and all time (omnipresent), and supports some organisation that is all-seeing and even all-knowing (omniscient)", which can be achieved through the use of embedded chips for instance (p. 33); *exaggerated surveillance*, referring to "the extent to which surveillance is undertaken... its justification is exaggerated" (p. 34) ; and/or *meta-, supra-, or master-surveillance*, which "could involve the consolidation of multiple surveillance threads in order to develop what would be envisaged by its proponents to be superior information" (p. 38). Shay et al. (2012) acknowledge:

> *"The pervasive nature of sensors coupled with recent advances in data mining, networking, and storage technologies creates tools and data that, while serving the public good, also create a ubiquitous surveillance infrastructure ripe for misuse. Roger Clarke's concept of dataveillance and M.G. Michael and Katina Michael's more recent uberveillance serve as important milestones in awareness of the growing threat of our instrumented world."*

All of these definitions indicate direct ways in which IoT applications can also be rolled-out whether it is for use of vehicle management in heavy traffic conditions, the tracking of suspects in a criminal investigation or even employees in a workplace. Disturbing is the manner in which a whole host of applications, particularly in tollways and public transportation, are being used for legal purposes without the knowledge of the driver and commuter. "Tapping" token cards is not only encouraged but mandatory at most metropolitan train stations of developed countries. Little do commuters know that the data gathered by these systems can be requested by a host of government agencies without a warrant.

Implications of überveillance on control

Irrespective of interpretation, the subject of current scholarly debate relates to the implications of überveillance on individuals in particular, and society in general. In an article discussing the evolution of automatic identification (auto-ID) techniques, Michael and Michael (2005) present an account of the issues associated with implantable technologies in humancentric applications. The authors note the evident trend of deploying a technology into the marketplace, prior to assessing the potential consequences (Michael and Michael 2005, pp. 22-33). This reactive approach causes apprehension in view of chip implants in particular, given the inexorable nature of embedded chips, and the fact that once the chip is accepted by the body, it is impossible to remove without an invasive surgical procedure, as summarised in the following excerpt:

> *"[U]nless the implant is removed within a short time, the body will adopt the foreign object and tie it to tissue. At this moment, there will be no exit strategy, no contingency plan, it will be a life enslaved to upgrades, virus protection mechanisms, and inescapable intrusion"* (Michael and Michael 2007, p. 18).

Other concerns relevant to this investigation have also been raised. It is indicated that "über-intrusive technologies" are likely to leave substantial impressions on individuals, families and other social relations, with the added potential of affecting psychological well-being (Michael and Michael 2007, p. 17). Apart from implications for individuals, concerns also emerge at the broader social level that require remedies. For instance, if a state of überveillance is to be avoided, caution must be exercised in deploying technologies without due reflection of the corresponding implications. Namely, this will involve the introduction of appropriate regulatory measures, which will encompass proactive consideration of the social implications of emerging technologies and individuals assuming responsibility for promoting regulatory measures (Michael and Michael 2007, p. 20). It will also require a measured attempt to achieve some form of "balance" (Clarke 2007a, p. 43). The implications of überveillance are of particular relevance to LBS regulatory discussions, given that "overarching location tracking and monitoring is leading toward a state of überveillance" (Michael and Michael 2011, p. 2). As such, research into LBS regulation in Australia must be sensitive to both the significance of LBS to überveillance and the anticipated trajectory of the latter.

Unfortunately the same cannot be said for IoT-specific regulation. IoT is a fluid concept, and in many ways IoT is nebulous. It is made up of a host of technologies that are being integrated and are converging together over time. It is layers upon layers of infrastructure which have emerged since the inception of the first telephone lines to the cloud and wireless Internet today. IoT requires new protocols and new applications but it is difficult to point to a specific technology or application or system that can be subject to some form of external oversight. Herein lie the problems of potential unauthorised disclosure of data, or even misuse of data when government agencies require private enterprise to act upon their requests, or private enterprises work together in sophisticated ways to exploit the consumer.

Comparing the different forms of 'veillance'

Various terms ending in 'veillance' have been introduced throughout this paper, all of which imply and encompass the process of monitoring. Prior to delving into the dangers of this activity and the significance of LBS monitoring on control, it is helpful to compare the main features of each term. A comparison of surveillance, dataveillance, sousveillance, and überveillance is provided in Table 2.

It should be noted that with the increased use of techniques such as surveillance, dataveillance, sousveillance and überveillance, the threat of becoming a *surveillance society* looms. According to Ganascia (2010p. 491), a surveillance society is one in which the data gathered from the aforementioned techniques is utilised to exert power and control over others. This results in dangers such as the potential for identification and profiling of individuals (Clarke 1997), the latter of which can be associated with social sorting (Gandy 1993).

Table 2: Comparison of the different forms of 'veillance'

Type of 'veillance'	Main systems/ technologies utilised	Primary focus
Surveillance	Visual monitoring systems	First hand observation/ images
Dataveillance	Automated, and therefore efficient, personal data collection systems	Data and aggregated data/information
Sousveillance	Wearable computing devices and technologies	Capture of audiovisual and sensory data, which may include location information
Überveillance	Embedded radio-frequency identification (RFID) chips	Identity and real-time location information

Identification

Identity and identification are ambiguous terms with philosophical and psychological connotations (Kodl and Lokay 2001, p. 129). Identity can be perceived as "a particular presentation of an entity, such as a role that the entity plays in particular circumstances" (Clarke and Wigan 2011). With respect to information systems, *human identification* specifically (as opposed to object identification) is therefore "the association of data with a particular human being" (Kodl and Lokay 2001, pp. 129-130). Kodl and Lokay (2001, pp. 131-135) claim that numerous methods exist to identify individuals prior to performing a data linkage, namely, using appearance, social interactions/behaviours, names, codes and knowledge, amongst other techniques. With respect to LBS, these *identifiers* significantly contribute to the dangers pertaining to surveillance, dataveillance, souseveillance and überveillance. That is, LBS can be deployed to simplify and facilitate the process of tracking and be used

for the collection of profile data that can potentially be linked to an entity using a given identification scheme. In a sense, LBS in their own right become an additional form of identification feeding the IoT scheme (Michael and Michael, 2013).

Thus, in order to address the regulatory concerns pertaining to LBS, it is crucial to appreciate the challenges regarding the identification of individuals. Of particularly importance is recognition that once an individual has been identified, they can be subjected to varying degrees of control. As such, in any scheme that enables identification, Kodl and Lokay (2001, p. 136) note the need to balance human rights with other competing interests, particularly given that identification systems may be exploited by powerful entities for control purposes, such as by governments to exercise social control. For an historical account of identification techniques, from manual methods through to automatic identification systems including those built on LBS see Michael and Michael (2009, pp. 43-60). It has also been suggested that civil libertarians and concerned individuals assert that automatic identification (auto-ID) technology "impinges on human rights, the right to privacy, and that eventually it will lead to totalitarian control of the populace that have been put forward since at least the 1970s" (Michael and Michael 2009, p. 364). These views are also pertinent to the notion of *social sorting*.

Social sorting

In relation to the theme of control, information derived from surveillance, dataveillance, sousveillance and überveillance techniques can also serve the purpose of social sorting, labelled by Oscar Gandy (1993, p. 1) as the "panoptic sort." Relevant to this discussion, the information may relate to an individual's location. In Gandy's influential work *The Panoptic Sort: A Political Economy of Personal Information*, the author relies on the work of Michel Foucault and other critical theorists (refer to pp. 3-13) in examining the panoptic sort as an "antidemocratic system of control" (Gandy 1993, p. 227). According to Gandy, in this system, individuals are exposed to prejudiced forms of categorisation based on both economic and political factors (pp. 1-2). Lyon (1998, p. 94) describes the database management practices associated with social sorting, classing them a form of *consumer surveillance*, in which customers are grouped by "social type and location." Such clustering forms the basis for the exclusion and marginalisation of individuals (King 2001, pp. 47-49). As a result, social sorting is presently used for profiling of individuals and in the market research realm (Bennett and Regan 2004, p. 452).

Profiling

Profiling "is a technique whereby a set of characteristics of a particular class of person is inferred from past experience, and data-holdings are then searched for individuals with a close fit to that set of characteristics" (Clarke 1993). The process is centred on the creation of a profile or model related to a specific individual, based on data aggregation processes (Casal 2004, p. 108). Assorted terms have been employed in labelling this profile. For instance, the model created of an individual using the data collected through dataveillance techniques has been referred to by Clarke (1997) as "the digital persona", and is related to the "digital dossiers" idea introduced by Solove (2004, pp. 1-7). According to Clarke (1994), the use of networked systems, namely the internet, involves communicating and exposing data and certain aspects of, at times, recognisable behaviour, both of which are utilised in the creation of a personality.

Digital personas and dossiers

The resulting personality is referred to as the digital persona. Similarly, *digital dossiers* refer to the compilation of comprehensive electronic data related to an individual, utilised in the creation of the "digital person" (Solove 2004, p. 1), also referred to as "digital biographies" (Solove 2002, p. 1086). Digital biographies are further discussed by Solove (2002). In examining the need for LBS regulation throughout the globe, a given regulatory response or framework must appreciate the ease with which (past, present and future) location information can be compiled and integrated into an individual's digital persona or dossier. Once such information is reproduced and disseminated the control implications are magnified.

With respect to the theme of control, an individual can exercise a limited amount of influence over their digital persona, as some aspects of creating an electronic personality may not be within their direct control. The scope of this article does not allow for reflection on the digital persona in great detail; however, Clarke (1994) offers a thorough investigation of the term, and associated notions such as the passive and active digital persona, in addition to the significance of the digital person to dataveillance techniques such as computer matching and profiling. However, significant to this research is the distinction between the physical and the digital persona and the resultant implications in relation to control, as summarised in the following extract:

> *"The physical persona is progressively being replaced by the digital persona as the basis for social control by governments, and for consumer marketing by corporations. Even from the strictly social control and business efficiency perspectives, substantial flaws exist in this approach. In addition, major risks to individuals and society arise"* (Clarke 1994).

The same sentiments apply with respect to digital dossiers. In particular, Solove (2004, p. 2) notes that individuals are unaware of the ways in which their electronic data is exploited by government and commercial entities, and "lack the power to do much about it." It is evident that profile data is advantageous for both social control and commercial purposes (Clarke 2001d, p. 12), the latter of which is associated with market research and sorting activities, which have evolved from ideas of "containment" of mobile consumer demand to the "control" model (Arvidsson 2004, pp. 456, 458-467). The control model in particular has been strengthened, but not solely driven, by emerging technologies including LBS, as explained:

> *"The control paradigm thus permits a tighter and more efficient surveillance that makes use of consumer mobility rather than discarding it as complexity. This ability to follow the consumer around has been greatly strengthened by new technologies: software for data mining, barcode scans, internet tracking devices, and lately location based information from mobile phones" (*Arvidsson 2004, p. 467).

Social sorting, particularly for profiling and market research purposes, thus introduces numerous concerns relating to the theme of control, one of which is the ensuing consequences relating to personal privacy. This specifically includes the privacy of location information. In sum, examining the current regulatory framework for LBS in Australia, and determining the need for LBS regulation, necessitates an appreciation of the threats associated with social sorting using information derived from LBS solutions. Additionally, the benefits and risks associated with surveillance, dataveillance, sousveillance and überveillance for control must be measured and carefully contemplated in the proposed regulatory response.

Trust

Trust is a significant theme relating to LBS, given the importance of the notion to: (a) "human existence" (Perusco et al. 2006, p. 93; Perusco and Michael 2007, p. 10), (b) relationships (Lewis and Weigert 1985, pp. 968-969), (c) intimacy and rapport within a domestic relationship (Boesen et al. 2010, p. 65), and (d) LBS success and adoption (Jorns and Quirchmayr 2010, p. 152). Trust can be defined, in general terms, as the "firm belief in the reliability, truth, or ability of someone or something" (Oxford Dictionary 2012b). A definition of trust that has been widely cited in relevant literature is "the willingness of a party to be vulnerable to the actions of another party based on the expectation that the other will perform a particular action important to the trustor, irrespective of the ability to monitor or control that other party" (Mayer et al. 1995, p. 712). Related to electronic relationships or transactions, the concept has been defined as the "confident reliance by one party on the behaviour of other parties" (Clarke 2001c, p. 291), and it has been suggested that in the electronic-commerce domain, in particular, trust is intimately associated with the disclosure of information (Metzger 2004).

In reviewing literature concerning trust, Fusco et al. (2011, p. 2) claim that trust is typically described as a dynamic concept falling into the categories of cognitive (evidence based), emotional (faith-based), and/or behavioural (conduct-based) trust. For further reading, the major sources on trust can be found in: Lewis and Weigert's (1985) sociological treatment of trust, the influential work of Mayer et al. (1995) and the authors' updated work Schoorman et al. (2007) centred on organisational trust, Weckert's (2000) comprehensive review

of trust in the context of workplace monitoring using electronic devices, research on trust in electronic-commerce (refer to McKnight and Chervany 2001; Pavlou 2003; Kim et al. 2009) and mobile-commerce (see Siau and Shen 2003; Yeh and Li 2009), the work of Valachich (2003) that introduces and evaluates trust in terms of ubiquitous computing environments, Dwyer et al.'s (2007) article on trust and privacy issues in social networks, Yan and Holtmanns' (2008) examination of issues associated with digital trust management, the work of Chen et al. (2008) covering the benefits and concerns of LBS usage including privacy and trust implications, and the research by Junglas and Spitzmüller (2005) that examines privacy and trust issues concerning LBS by presenting a research model that incorporates these aspects amongst others.

For the purpose of this paper, the varying definitions and categorisations are acknowledged. However, trust will be assessed in terms of the relationships dominating existing LBS/IoT scholarship which comprise the government-citizen relationship centred on trust in the state, the business-consumer relationship associated with trust in corporations/LBS providers, and the consumer-consumer relationship concerned with trust in individuals/others.

Trust in the state

Trust in the state broadly covers LBS solutions implemented by government, thus representing the government-citizen relationship. Dominating current debates and literature are LBS government initiatives in the form of emergency management schemes, in conjunction with national security applications utilising LBS, which depending on the nature of their implementation may impact on citizens' trust in the state. These concerns are typically expressed as a trade-off between security and safety. At present there are very few examples of fully-fledged IoT systems to point to, although increasingly quasi-IoT systems are being deployed using wireless sensor networks of varying kinds, e.g. for bushfire management and for fisheries. These systems do not include a direct human stakeholder but are still relevant as they may trigger flow-on effects that do impact citizenry.

Balancing trust and privacy in emergency services

In the context of emergency management, Aloudat and Michael (2011, p. 58) maintain that the dominant theme between government and consumers in relation to emergency warning messages and systems is trust. This includes trust in the LBS services being delivered and in the government itself (Aloudat and Michael 2011, p. 71). While privacy is typically believed to be the leading issue confronting LBS, in emergency and life-threatening situations it is overwhelmed by trust-related challenges, given that users are generally willing to relinquish their privacy in the interest of survival (Aloudat and Michael 2010, p. 2). Furthermore, the success of these services is reliant on trust in the technology, the service, and the accuracy/reliability/timeliness of the emergency alert. On the whole, this success can be measured in terms of citizens' confidence in their government's ability to sensibly select and implement a fitting emergency service utilising enhanced LBS features. In a paper that examines the deployment of location services in Dutch public administration, van Ooijen and Nouwt (2009, p. 81) assess the impact of government-based LBS initiatives on the government-citizen relationship, recommending that governments employ care in gathering and utilising location-based data about the public, to ensure that citizens' trust in the state is not compromised.

Trust-related implications of surveillance in the interest of national security

Trust is also prevalent in discussions relating to national security. National security has been regarded a priority area for many countries for over a decade, and as such has prompted the implementation of surveillance schemes by government. Wigan and Clarke (2006, p. 392) discuss the dimension of trust as a significant theme contributing to the social acceptance of a particular government surveillance initiative, which may incorporate location and tracking of individuals and objects. The implementation of surveillance systems by the state, including those incorporating LBS, can diminish the public's confidence in the state given the potential for such mechanisms to be perceived as a form of authoritarian control. Nevertheless, a situation where national security

and safety are considered to be in jeopardy may entail (partial) acceptance of various surveillance initiatives that would otherwise be perceived objectionable. In such circumstances, trust in government plays a crucial role in determining individuals' willingness to compromise various civil liberties. This is explained by Davis and Silver (2004, p. 35) below:

> *"The more people trust the federal government or law enforcement agencies, the more willing they are to allow the government leeway in fighting the domestic war on terrorism by conceding some civil liberties."*

However, in due course it is expected that such increased security measures (even if initially supported by citizens) will yield a growing gap between government and citizens, "potentially dampening citizen participation in government and with it reducing citizens' trust in public institutions and officials" (Gould 2002, p. 77). This is so as the degree of threat and trust in government is diminishing, thus resulting in the public's reluctance to surrender their rights for the sake of security (Sanquist et al. 2008, p. 1126). In order to build and maintain trust, governments are required to be actively engaged in developing strategies to build confidence in both their abilities and of the technology under consideration, and are challenged to recognise "the massive harm that surveillance measures are doing to public confidence in its institutions" (Wigan and Clarke 2006, p. 401). It has been suggested that a privacy impact assessment (PIA) aids in establishing trust between government and citizens (Clarke 2009, p. 129). Carefully considered legislation is an alternative technique to enhance levels of trust. With respect to LBS, governments are responsible for proposing and enacting regulation that is in the best interest of citizens, incorporating citizen concerns into this process and encouraging suitable design of LBS applications, as explained in the following quotation:

> *"...new laws and regulations must be drafted always on the basis of citizens' trust in government authorities. This means that citizens trust the government to consider the issues at stake according to the needs and wishes of its citizens. Location aware services can influence citizens' trust in the democratic society. Poorly designed infrastructures and services for storing, processing and distributing location-based data can give rise to a strong feeling of being threatened. Whereas a good design expands the feeling of freedom and safety, both in the private and in the public sphere/domain"* (Beinat et al. 2007, p. 46).

One of the biggest difficulties that will face stakeholders is identifying when current LBS systems become a part of bigger IoT initiatives. Major changes in systems will require a re-evaluation of impact assessments of different types.

Need for justification and cultural sensitivity

Techniques of this nature will fail to be espoused, however, if surveillance schemes lack adequate substantiation at the outset, as trust is threatened by "absence of justification for surveillance, and of controls over abuses" (Wigan and Clarke 2006, p. 389). From a government perspective, this situation may prove detrimental, as Wigan and Clarke (2006, p. 401) claim that transparency and trust are prerequisites for ensuring public confidence in the state, noting that "[t]he integrity of surveillance schemes, in transport and elsewhere, is highly fragile." Aside from adequate justification of surveillance schemes, cultural differences associated with the given context need to be acknowledged as factors influencing the level of trust citizens hold in government. As explained by Dinev et al. (2005, p. 3) in their cross-cultural study of American and Italian Internet users' privacy and surveillance concerns, "[a]ttitudes toward government and government initiatives are related to the culture's propensity to trust." In comparing the two contexts, Dinev et al. claim that Americans readily accept government surveillance to provide increased levels of security, whereas Italians' low levels of trust in government results in opposing viewpoints (pp. 9-10).

Trust in corporations/LBS/IoT providers

Trust in corporations/LBS/IoT providers emerges from the level of confidence a user places in an organisation and their respective location-based solution(s), which may be correlated to the business-consumer relationship. In the context of consumer privacy, Culnan and Bies (2003, p. 327) assert that perceived trust in an organisation is closely linked to the extent to which an organisation's practices are aligned with its policies. A breach in this trust affects the likelihood of personal information disclosure in the future (Culnan and Bies 2003, p. 328), given the value of trust in sustaining lasting customer relationships (p. 337). Reducing this "trust gap" (Culnan and Bies 2003, pp. 336-337) is a defining element for organisations in achieving economic and industry success, as it may impact on a consumer's decision to contemplate location data usage (Chen et al. 2008, p. 34). Reducing this gap requires that control over location details remain with the user, as opposed to the LBS provider or network operator (Giaglis et al. 2003, p. 82). Trust can thus emerge from a user's perception that they are in command (Junglas and Spitzmüller 2005, p. 3).

Küpper and Treu (2010, pp. 216-217) concur with these assertions, explaining that the lack of uptake of first-generation LBS applications was chiefly a consequence of the dominant role of the network operator over location information. This situation has been somewhat rectified since the introduction of GPS-enabled devices capable of determining location information without input from the network operator and higher emphasis on a user-focussed model (Bellavista et al. 2008, p. 85; Küpper and Treu 2010, p. 217). Trust, however, is not exclusively concerned with a network operator's ability to determine location information, but also with the possible misuse of location data. As such, it has also been framed as a potential resolution to location data misappropriation, explained further by Jorns and Quirchmayr (2010, p. 152) in the following excerpt:

> *"The only way to completely avoid misuse is to entirely block location information, that is, to reject such services at all. Since this is not an adequate option... trust is the key to the realization of mobile applications that exchange sensitive information."*

There is much to learn from the covert and overt location tracking of large corporation on their subscribers. Increasingly, the dubious practices of retaining location information by information and communication technology giants Google, Apple and Microsoft are being reported and only small commensurate penalties being applied in countries in the European Union and Asia. Disturbing in this trend is that even smaller suppliers of location-based applications are beginning to unleash unethical (but seemingly not illegal) solutions at shopping malls and other campus-based locales (Michael & Clarke 2013).

Importance of identity and privacy protection to trust

In delivering trusted LBS solutions, Jorns and Quirchmayr (2010, pp. 151-155) further claim that identity and privacy protection are central considerations that must be built into a given solution, proposing an LBS architecture that integrates such safeguards. That is, identity protection may involve the use of false dummies, dummy users and landmark objects, while privacy protection generally relies on decreasing the resolution of location data, employing supportive regulatory techniques and ensuring anonymity and pseudonymity (Jorns and Quirchmayr 2010, p. 152). Similarly, and with respect to online privacy, Clarke (2001c, p. 297) suggests that an adequate framework must be introduced that "features strong and comprehensive privacy laws, and systematic enforcement of those laws." These comments, also applicable to LBS in a specific sense, were made in the context of economic rather than social relationships, referring primarily to government and corporations, but are also relevant to trust amongst social relations.

It is important to recognise that issues of trust are closely related to privacy concerns from the perspective of users. In an article titled, "Trust and Transparency in Location-Based Services: Making Users Lose their Fear of Big Brother", Böhm et al. (2004, pp. 1-3) claim that operators and service providers are charged with the difficult task of earning consumer trust and that this may be achieved by addressing user privacy concerns and adhering to relevant legislation. Additional studies also point to the relationship between trust and privacy, claiming that trust can aid in reducing the perceived privacy risk for users. For example, Xu et al. (2005) suggest

that enhancing trust can reduce the perceived privacy risk. This influences a user's decision to disclose information, and that "service provider's interventions including joining third party privacy seal programs and introducing device-based privacy enhancing features could increase consumers' trust beliefs and mitigate their privacy risk perceptions" (Xu et al. 2005, p. 905). Chellappa and Sin (2005, pp. 188-189), in examining the link between trust and privacy, express the importance of trust building, which include consumer's familiarity and previous experience with the organisation.

Maintaining consumer trust

The primary consideration in relation to trust in the business-consumer relationship is that all efforts be targeted at establishing and building trust in corporations and LBS/IoT providers. Once trust has been compromised, the situation cannot be repaired which is a point applicable to trust in any context. This point is explained by Kaasinen (2003, p. 77) in an interview-based study regarding user requirements in location-aware mobile applications:

> *"The faith that the users have in the technology, the service providers and the policy-makers should be regarded highly. Any abuse of personal data can betray that trust and it will be hard to win it back again."*

Trust in individuals/others

Trust in the consumer-to-consumer setting is determined by the level of confidence existing between an individual and their social relations, which may include *friends, parents, other family members, employers* and *strangers*, categories that are adapted from Levin et al. (2008, pp. 81-82). Yan and Holtmanns (2008, p. 2) express the importance of trust for social interactions, claiming that "[s]ocial trust is the product of past experiences and perceived trustworthiness." It has been suggested that LBS monitoring can erode trust between the individual engaged in monitoring and the subject being monitored, as the very act implies that trust is lacking in a given relationship (Perusco et al. 2006, p. 93). These concerns are echoed in Michael et al. (2008). Previous studies relevant to LBS and trust generally focus on: the workplace situation, that is, trust between an employer and their employee; trust amongst 'friends' subscribed to a location-based social networking (LBSN) service which may include any of the predefined categories above; in addition to studies relating to the tracking of family members, such as children for instance, for safety and protection purposes and the relative trust implications.

Consequences of workplace monitoring

With respect to trust in an employer's use of location-based applications and location data, a prevailing subject in existing literature is the impact of employee monitoring systems on staff. For example, in studying the link between electronic workplace monitoring and trust, Weckert (2000, p. 248) reported that trust is a significant issue resulting from excessive monitoring, in that monitoring may contribute to deterioration in professional work relationships between an employer and their employee and consequently reduce or eliminate trust. Weckert's work reveals that employers often substantiate electronic monitoring based on the argument that the "benefits outweigh any loss of trust", and may include gains for the involved parties; notably, for the employer in the form of economic benefits, for the employee to encourage improvements to performance and productivity, and for the customer who may experience enhanced customer service (p. 249). Chen and Ross (2005, p. 250), on the other hand, argue that an employer's decision to monitor their subordinates may be related to a low degree of existing trust, which could be a result of unsuitable past behaviour on the part of the employee. As such, employers may perceive monitoring as necessary in order to manage employees. Alternatively, from the perspective of employees, trust-related issues materialise as a result of monitoring, which may leave an impression on job attitudes, including satisfaction and dedication, as covered in a paper by Alder et al. (2006) in the context of internet monitoring.

When applied to location monitoring of employees using LBS, the trust-related concerns expressed above are indeed warranted. Particularly, Kaupins and Minch (2005, p. 2) argue that the appropriateness of location monitoring in the workplace can be measured from either a legal or ethical perspective, which inevitably results in policy implications for the employer. The authors emphasise that location monitoring of employees can often be justified in terms of the security, productivity, reputational and protective capabilities of LBS (Kaupins and Minch 2005, p. 5). However, Kaupins and Minch (2005, pp. 5-6) continue to describe the ethical factors "limiting" location monitoring in the workplace, which entail the need for maintaining employee privacy and the restrictions associated with inaccurate information, amongst others. These factors will undoubtedly affect the degree of trust between an employer and employee.

However, the underlying concern relevant to this discussion of location monitoring in the workplace is not only the suitability of employee monitoring using LBS. While this is a valid issue, the challenge remains centred on the deeper trust-related consequences. Regardless of the technology or applications used to monitor employees, it can be concluded that a work atmosphere lacking trust results in sweeping consequences that extend beyond the workplace, expressed in the following excerpt:

> *"A low trust workplace environment will create the need for ever increasing amounts of monitoring which in turn will erode trust further. There is also the worry that this lack of trust may become more widespread. If there is no climate of trust at work, where most of us spend a great deal of our life, why should there be in other contexts? Some monitoring in some situations is justified, but it must be restricted by the need for trust"* (Weckert 2000, p. 250).

Location-monitoring amongst friends

Therefore, these concerns are certainly applicable to the use of LBS applications amongst other social relations. Recent literature merging the concepts of LBS, online social networking and trust are particularly focused on the use of LBSN applications amongst various categories of *friends*. For example, Fusco et al.'s (2010) qualitative study examines the impact of LBSN on trust amongst friends, employing a focus group methodology in achieving this aim. The authors reveal that trust may suffer as a consequence of LBSN usage in several ways: as disclosure of location information and potential monitoring activities can result in application misuse in order to conceal things; excessive questioning and the deterioration in trust amongst social relations; and trust being placed in the application rather than the friend (Fusco et al. 2010, p. 7). Further information relating to Fusco et al.'s study, particularly the manner in which LBSN applications adversely impact on trust can be found in a follow-up article (Fusco et al. 2011).

Location tracking for protection

It has often been suggested that monitoring in familial relations can offer a justified means of protection, particularly in relation to vulnerable individuals such as Alzheimer's or dementia sufferers and in children. With specific reference to the latter, trust emerges as a central theme relating to child tracking. In an article by Boesen et al. (2010) location tracking in families is evaluated, including the manner in which LBS applications are incorporated within the familial context. The qualitative study conducted by the authors revealed that the initial decision to use LBS by participants with children was a lack of existing trust within the given relationship, with participants reporting an improvement in their children's behaviour after a period of tracking (Boesen et al. 2010, p. 70). Boesen et al., however, warn of the trust-related consequences, claiming that "daily socially-based trusting interactions are potentially replaced by technologically mediated interactions" (p. 73). Lack of trust in a child is considered to be detrimental to their growth. The act of nurturing a child is believed to be untrustworthy through the use of technology, specifically location monitoring applications, may result in long-term implications. The importance of trust to the growth of a child and the dangers associated with ubiquitous forms of supervision are explained in the following excerpt:

> *"Trust (or at least its gradual extension as the child grows) is seen as fundamental to emerging self-control and healthy development... Lack of private spaces (whether physical, personal or social) for*

children amidst omni-present parental oversight may also create an inhibiting dependence and fear" (Marx and Steeves 2010, p. 218).

Furthermore, location tracking of children and other individuals in the name of protection may result in undesirable and contradictory consequences relevant to trust. Barreras and Mathur (2007, p. 182), in an article that describes the advantages and disadvantages of wireless location tracking, argue that technologies originally intended to protect family members (notably children, and other social relations such as friends and employees), can impact on trust and be regarded as "unnecessary surveillance." The outcome of such tracking and reduced levels of trust may also result in a "counterproductive" effect if the tracking capabilities are deactivated by individuals, rendering them incapable of seeking assistance in actual emergency situations (Barreras and Mathur 2007, p. 182).

LBS/IoT is a 'double-edged sword'

In summary, location monitoring and tracking by the state, corporations and individuals is often justified in terms of the benefits that can be delivered to the party responsible for monitoring/tracking and the subject being tracked. As such, Junglas and Spitzmüller (2005, p. 7) claim that location-based services can be considered a "double-edged sword" in that they can aid in the performance of tasks in one instance, but may also generate Big Brother concerns. Furthermore, Perusco and Michael (2007, p. 10) mention the linkage between trust and freedom. As a result, Perusco et al. (2006, p. 97) suggest a number of questions that must be considered in the context of LBS and trust: "Does the LBS context already involve a low level of trust?"; "If the LBS context involves a moderate to high level of trust, why are LBS being considered anyway?"; and "Will the use of LBS in this situation be trust-building or trust-destroying?" In answering these questions, the implications of LBS/IoT monitoring on trust must be appreciated, given they are significant, irreparable, and closely tied to what is considered the central challenge in the LBS domain, privacy.

This paper has provided comprehensive coverage of the themes of control and trust with respect to the social implications of LBS. The subsequent discussion will extend the examination to cover LBS in the context of the IoT, providing an ethical analysis and stressing the importance of a robust socio-ethical framework.

Discussion

The Internet of Things (IoT) and LBS: extending the discussion on control and trust

The Internet of Things (IoT) is an encompassing network of connected intelligent "things", and is "comprised of smart machines interacting and communicating with other machines, objects, environments and infrastructures" (Freescale Semiconductor Inc. and ARM Inc. 2014, p. 1). The phrase was originally coined by Kevin Ashton in 1999, and a definite definition is yet to be agreed upon (Ashton 2009, p. 1; Kranenburg and Bassi 2012, p. 1). Various forms of IoT are often used interchangeably, such as the Internet of Everything, the Internet of Things and People, the Web of Things and People etc. The IoT can, however, be described in terms of its core characteristics and/or the features it encompasses. At the crux of the IoT concept is the integration of the physical and virtual worlds, and the capability for "things" within these realms to be operated remotely through the employment of intelligent or smart objects with embedded processing functionality (Mattern and Floerkemeier 2010, p. 242; Ethics Subgroup IoT 2013, p. 3). These smart objects are capable of storing historical and varied forms of data, used as the basis for future interactions and the establishment of preferences. That is, once the data is processed, it can be utilized to "command and control" things within the IoT ecosystem, ideally resulting in enhancing the everyday lives of individual (Michael, K. et al., 2010).

According to Ashton (2009, p. 1), the IoT infrastructure should "empower computers" and exhibit less reliance on human involvement in the collection of information. It should also allow for "seamless" interactions and connections (Ethics Subgroup IoT 2013, p. 2). Potential use cases include personal/home applications,

health/patient monitoring systems, and remote tracking and monitoring which may include applications such as asset tracking amongst others (Ethics Subgroup IoT 2013, p. 3).

As can be anticipated with an ecosystem of this scale, the nature of interactions with the physical/virtual worlds and the varied "things" within, will undoubtedly be affected and dramatically alter the state of play. In the context of this paper, the focus is ultimately on the ethical concerns emerging from the use of LBS within the IoT infrastructure that is characterized by its ubiquitous/pervasive nature, in view of the discussion above regarding control and trust. It is valuable at this point to identify the important role of LBS in the IoT infrastructure.

While the IoT can potentially encompass a myriad of devices, the mobile phone will likely feature as a key element within the ecosystem, providing connectivity between devices (Freescale Semiconductor Inc. and ARM Inc. 2014, p. 2). In essence, smart phones can therefore be perceived as the "mediator" between users, the internet and additional "things", as is illustrated in Mattern and Floerkemeier (2010, p. 245, see figure 2). Significantly, most mobile devices are equipped with location and spatial capabilities, providing "localization", whereby intelligent devices "are aware of their physical location, or can be located" (Mattern and Floerkemeier 2010, p. 244). An example of an LBS application in the IoT would be indoor navigation capabilities in the absence of GPS; or in affect seamless navigation between the outdoor and indoor environments.

Control- and trust-related challenges in the IoT

It may be argued that the LBS control and trust implications discussed throughout this paper (in addition to ethical challenges such as privacy and security) will matriculate into the IoT environment. However, it has also been suggested that "the IoT will essentially create much richer environments in which location-based and location-aware technology can function" (Blouin 2014), and in doing so the ethical challenges will be amplified. It has further been noted that ethical issues, including trust and control amongst others, will "gain a new dimension in light of the increased complexity" in the IoT environment (Ethics Subgroup IoT 2013, p. 2).

In relation to control and the previously identified surveillance metaphors, for instance, it is predicted that there will be less reliance on Orwell's notion of Big Brother whereby surveillance is conducted by a single entity. Rather the concept of "some brother" will emerge. Some brother can be defined as "a heterogeneous 'mass' consisting of innumerable social actors, e.g. public sector authorities, citizens' movements and NGOs, economic players, big corporations, SMEs and citizens" (Ethics Subgroup IoT 2013, p. 16). As can be anticipated, the ethical consequences and dangers can potentially multiply in such a scenario.

Following on from this idea, is that of lack of transparency. The IoT will inevitably result in the merging of both the virtual and physical worlds, in addition to public and private spaces. It has been suggested that lack of transparency regarding information access will create a sense of discomfort and will accordingly result in diminishing levels of trust (Ethics Subgroup IoT 2013, p. 8). The trust-related issues (relevant to LBS) are likely to be consistent with those discussed throughout this paper, possibly varying in intensity/severity depending on a given scenario. For example, the consequences of faulty IoT technology have the potential to be greater than those in conventional Internet services given the integration of the physical and virtual worlds, thereby impact on users' trust in the IoT (Ethics Subgroup IoT 2013, p. 11). Therefore, trust considerations must primarily be examined in terms of: (a) trust in technology, and (b) trust in individuals/others.

Dealing with these (and other) challenges requires an ethical analysis in which appropriate conceptual and practical frameworks are considered. A preliminary examination is provided in the subsequent section, followed by dialogue regarding the need for objectivity in socio-ethical studies and the associated difficulties in achieving this.

Ethical analysis: proposing a socio-ethical conceptual framework

Research into the social and ethical implications of LBS, emerging technologies in general, and the IoT can be categorized in many ways and many frameworks can be applied. For instance, it may be regarded as a strand of "cyberethics", defined by Tavani (2007, p. 3) as "the study of moral, legal and social issues involving cybertechnology". Cybertechnology encompasses technological devices ranging from individual computers through to networked information and communication technologies. When considering ethical issues relating to cybertechnology and technology in general, Tavani (2007, pp. 23-24) notes that the latter should not necessarily be perceived as neutral. That is, technology may have "embedded values and biases" (Tavani 2007, p. 24), in that it may inherently provide capabilities to individuals to partake in unethical activities. This sentiment is echoed by Wakunuma and Stahl (2014, p. 393) in a paper examining the perceptions of IS professionals in relation to emerging ethical concerns.

Alternatively, research in this domain may be classed as a form of "computer ethics" or "information ethics", which can be defined and applied using numerous approaches. While this article does not attempt to provide an in-depth account of information ethics, a number of its crucial characteristics are identified. In the first instance, the value of information ethics is in its ability to provide a conceptual framework for understanding the array of ethical challenges stemming from the introduction of new ICTs (Mathiesen 2004, p. 1). According to Floridi (1999), the question at the heart of information ethics is "what is good for an information entity and the infosphere in general?" The author continues that "more analytically, we shall say that [information ethics] determines what is morally right or wrong, what ought to be done, what the duties, the 'oughts' and the 'ought nots' of a moral agent are…" However, Capurro (2006, p. 182) disagrees, claiming that information ethics is additionally about "what is good for our bodily being-in-the-world with others in particular?" This involves contemplation of other "spheres" such as the ecological, political, economic, and cultural and is not limited to a study of the infosphere as suggested by Floridi. In this sense, the significance of context, environment and intercultural factors also becomes apparent.

Following on from these notions, there is the need for a robust ethical framework that is multi-dimensional in nature and explicitly covers the socio-ethical challenges emerging from the deployment of a given technology. This would include, but not be limited to, the control and trust issues identified throughout this paper, other concerns such as privacy and security, and any challenges that emerge as the IoT takes shape. This article proposes a broader more robust socio-ethical conceptual framework, as an appropriate means of examining and addressing ethical challenges relevant to LBS; both LBS in general and as a vital mediating component within the IoT. This framework is illustrated in Figure 1. Central to the socio-ethical framework is the contemplation of individuals as part of a broader social network or society, whilst considering the interactions amongst various elements of the overall "system". The four themes underpinning socio-ethical studies include the investigation of what the human purpose is, what is moral, how justice is upheld and the principles that guide the usage of a given technique. Participants; their interactions with systems; people concerns and behavioural expectations; cultural and religious belief; structures, rules and norms; and fairness, personal benefits and personal harms are all areas of interest in a socio-ethical approach.

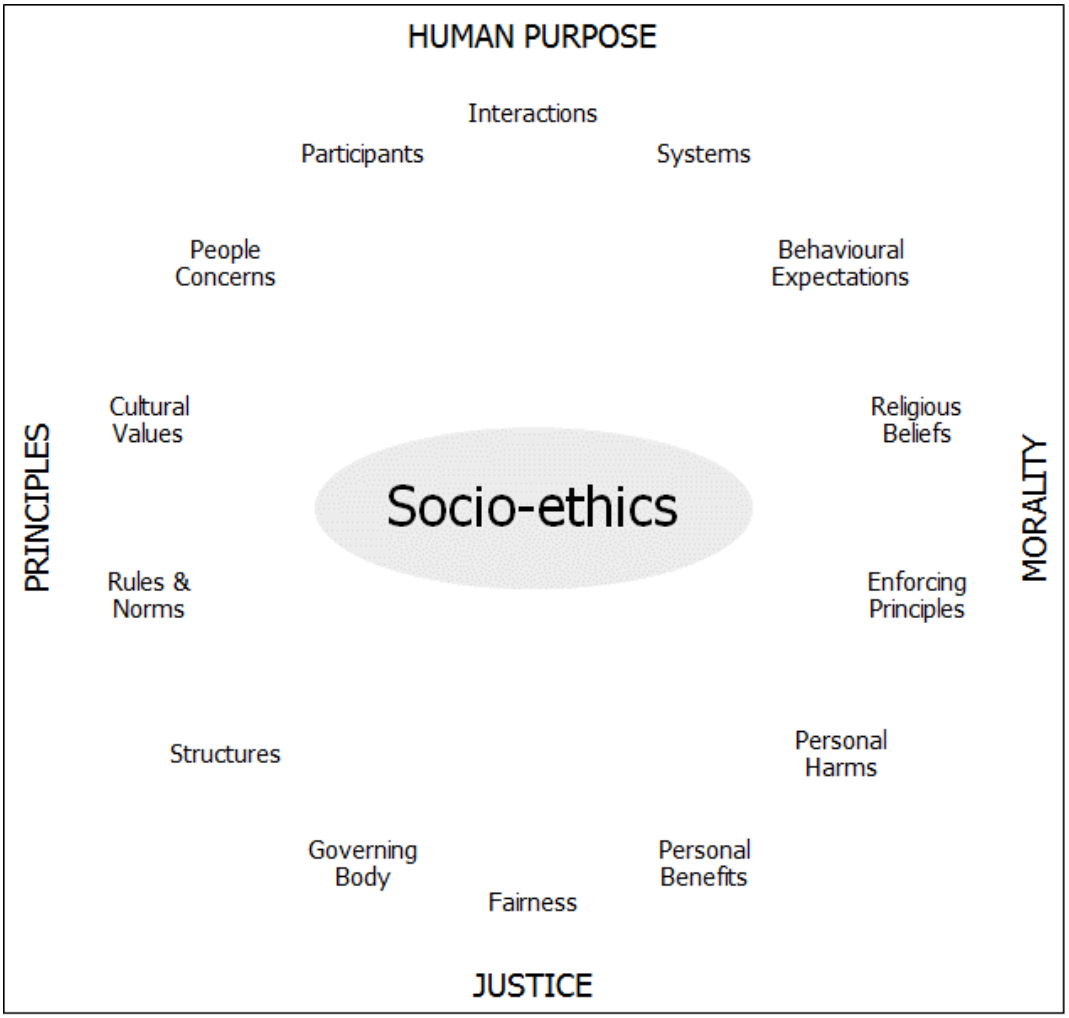

Figure 1: Proposed socio-ethical framework, in terms of the major components that require consideration

This article is intended to offer a preliminary account of the socio-ethical conceptual framework being proposed. Further research would examine and test its validity, whilst also providing a more detailed account of the various components within and how a socio-ethical assessment would be conducted based on the framework, and the range of techniques that could be applied.

The need for objectivity

Regardless of categorization and which conceptual framework is adopted, numerous authors stress that the focus of research and debates should not be skewed towards the unethical uses of a particular technology, but rather an objective stance should be embraced. Such objectivity must nonetheless ensure that social interests are adequately represented. That is, with respect to location and tracking technologies, Clarke (2001b, p. 220) claims that social interests have been somewhat overshadowed by the economic interests of LBS organisation. This is a situation that requires rectifying. While information technology professionals are not necessarily liable for how technology is deployed, they must nonetheless recognise its implications and be engaged in the process of introducing and promoting adequate safeguards (Clarke 1988, pp. 510-511). It has been argued that IS professionals are generally disinterested in the ethical challenges associated with emerging ICTs, and are rather concerned with the job or the technologies themselves (Wakunuma and Stahl 2014, p. 383).

This is explicitly the case for LBS given that the industry and technology have developed quicker than equivalent social implications scholarship and research, an unfavourable situation given the potential for LBS to have

profound impacts on individuals and society (Perusco et al. 2006, p. 91). In a keynote address centred on defining the emerging notion of überveillance, Clarke (2007a, p. 34) discusses the need to measure the costs and disbenefits arising from surveillance practices in general, where costs refer to financial measures, and disbenefits to all non-economic impacts. This involves weighing the negatives against the potential advantages, a response that is applicable to LBS, and pertinent to seeking objectivity.

Difficulties associated with objectivity

However, a major challenge with respect to an impartial approach for LBS is the interplay between the constructive and the potentially damaging consequences that the technology facilitates. For instance, and with specific reference to wireless technologies in a business setting, Elliot and Phillips (2004, p. 474) maintain that such systems facilitate monitoring and surveillance which can be applied in conflicting scenarios. Positive applications, according to Elliot and Phillips, include monitoring to improve effectiveness or provide employee protection in various instances, although this view has been frequently contested. Alternatively, negative uses involve excessive monitoring, which may compromise privacy or lead to situations in which an individual is subjected to surveillance or unauthorised forms of monitoring.

Additional studies demonstrate the complexities arising from the dual, and opposing, uses of a single LBS solution. It has been illustrated that any given application, for instance, parent, healthcare, employee and criminal tracking applications, can be simultaneously perceived as ethical and unethical (Michael et al. 2006a, p. 7). A closer look at the scenario involving parents tracking children, as explained by Michael et al. (2006a, p. 7), highlights that child tracking can enable the safety of a child on the one hand, while invading their privacy on the other. Therefore, the dual and opposing uses of a single LBS solution become problematic and situation-dependent, and indeed increasingly difficult to objectively examine. Dobson and Fischer (2003, p. 50) maintain that technology cannot be perceived as either good or evil in that it is not directly the cause of unethical behaviour, rather they serve to "empower those who choose to engage in good or bad behaviour."

This is similarly the case in relation to the IoT, as public approval of the IoT is largely centred on "the conventional dualisms of 'security versus freedom' and 'comfort versus data privacy'" (Mattern and Floerkemeier 2010, p. 256). Assessing the implications of the IoT infrastructure as a whole is increasingly difficult.

An alternative obstacle is associated with the extent to which LBS threaten the integrity of the individual. Explicitly, the risks associated with location and tracking technologies "arise from individual technologies and the trails that they generate, from compounds of multiple technologies, and from amalgamated and cross-referenced trails captured using multiple technologies and arising in multiple contexts" (Clarke 2001b, pp. 218). The consequent social implications or "dangers" are thus a product of individuals being convicted, correctly or otherwise, of having committed a particular action (Clarke 2001b, p. 219). A wrongly accused individual may perceive the disbenefits arising from LBS as outweighing the benefits.

However, in situations where integrity is not compromised, an LBS application can be perceived as advantageous. For instance, Michael et al. (2006, pp. 1-11) refer to the potentially beneficial uses of LBS, in their paper focusing on the Avian Flu Tracker prototype that is intended to manage and contain the spread of the infectious disease, by relying on spatial data to communicate with individuals in the defined location. The authors demonstrate that their proposed system which is intended to operate on a subscription or opt-in basis is beneficial for numerous stakeholders such as government, health organisations and citizens (Michael et al. 2006c, p. 6).

Thus, a common challenge confronting researchers with respect to the study of morals, ethics and technology is that the field of ethics is subjective. That is, what constitutes right and wrong behaviour varies depending on the beliefs of a particular individual, which are understood to be based on cultural and other factors specific to the individual in question. One such factor is an individual's experience with the technology, as can be seen in the previous example centred on the notion of an unjust accusation. Given these subjectivities and the potential for inconsistency from one individual to the next, Tavani (2007, p. 47) asserts that there is the need for ethical theories to direct the analysis of moral issues (relating to technology), given that numerous complications or disagreements exist in examining ethics.

Conclusion

This article has provided a comprehensive review of the control- and trust-related challenges relevant to location-based services, in order to identify and describe the major social and ethical considerations within each of the themes. The relevance of the IoT in such discussions has been demonstrated and a socio-ethical framework proposed to encourage discussion and further research into the socio-ethical implications of the IoT with a focus on LBS and/or localization technologies. The proposed socio-ethical conceptual framework requires further elaboration and it is recommended that a thorough analysis, beyond information ethics, be conducted based on this paper which forms the basis for such future work. IoT by its very nature is subject to socio-ethical dilemmas because for the greater part, the human is removed from decision-making processes and is instead subject to a machine.

References

Abbas, R., Michael, K., Michael, M.G. & Aloudat, A.: Emerging Forms of Covert Surveillance Using GPS-Enabled Devices. Journal of Cases on Information Technology 13(2), 2011, 19-33.

Albrecht, K. & McIntyre, L.: Spychips: How Major Corporations and Government Plan to Track Your Every Purchase and Watch Your Every Move. Tomas Nelson 2005.

Albrecht, K. & Michael, K.: Connected: To Everyone and Everything. IEEE Technology and Society Magazine, Winter, 2013, 31-34.

Alder, G.S., Noel, T.W. & Ambrose, M.L.: Clarifying the Effects of Internet Monitoring on Job Attitudes: The Mediating Role of Employee Trust. Information & Management, 43, 2006, 894-903.

Aloudat, A. & Michael, K.: The Socio-Ethical Considerations Surrounding Government Mandated Location-Based Services During Emergencies: An Australian Case Study, in M. Quigley (ed.), ICT Ethics and Security in the 21st Century: New Developments and Applications. IGI Global, Hershey, PA, 2010, 1-26.

Aloudat, A. & Michael, K.: Toward the Regulation of Ubiquitous Mobile Government: A case Study on Location-Based Emergency Services in Australia. Electronic Commerce Research, 11(1), 2011, 31-74.

Andrejevic, M.: ISpy: Surveillance and Power in the Interactive Era. University Press of Kansas, Lawrence, 2007.

Arvidsson, A.: On the 'Pre-History of the Panoptic Sort': Mobility in Market Research. Surveillance & Society, 1(4), 2004, 456-474.

Ashton, K.: The "Internet of Things" Things. RFID Journal, 2009, www.rfidjournal.com/articles/pdf?4986

Barreras, A. & Mathur, A.: Chapter 18. Wireless Location Tracking, in K.R. Larsen and Z.A. Voronovich (eds.), Convenient or Invasive: The Information Age. Ethica Publishing, United States, 2007, 176-186.

Bauer, H.H., Barnes, S.J., Reichardt, T. & Neumann, M.M.: Driving the Consumer Acceptance of Mobile Marketing: A Theoretical Framework and Empirical Study. Journal of Electronic Commerce Research, 6(3), 2005, 181-192.

Beinat, E., Steenbruggen, J. & Wagtendonk, A.: Location Awareness 2020: A Foresight Study on Location and Sensor Services. Vrije Universiteit, Amsterdam, 2007, http://reference.kfupm.edu.sa/content/l/o/location_awareness_2020_2_108_86452.pdf

Bellavista, P., Küpper, A. & Helal, S.: Location-Based Services: Back to the Future. IEEE Pervasive Computing, 7(2), 2008, 85-89.

Bennett, C.J. & Regan, P.M.: Surveillance and Mobilities. Surveillance & Society, 1(4), 2004, 449-455.

Bentham, J. & Bowring, J.: The Works of Jeremy Bentham. Published under the Superintendence of His Executor, John Bowring, Volume IV, W. Tait, Edinburgh, 1843.

Blouin, D. An Intro to Internet of Things. 2014, www.xyht.com/spatial-itgis/intro-to-internet-of-things/

Boesen, J., Rode, J.A. & Mancini, C.: The Domestic Panopticon: Location Tracking in Families. UbiComp'10, Copenhagen, Denmark, 2010, pp. 65-74.

Böhm, A., Leiber, T. & Reufenheuser, B.: 'Trust and Transparency in Location-Based Services: Making Users Lose Their Fear of Big Brother. Proceedings Mobile HCI 2004 Workshop On Location Systems Privacy and Control, Glasgow, UK, 2004, 1-4.

Capurro, R.: Towards an Ontological Foundation of Information Ethics. Ethics and Information Technology, 8, 2006, 175-186.

Casal, C.R.: Impact of Location-Aware Services on the Privacy/Security Balance, Info: the Journal of Policy, Regulation and Strategy for Telecommunications. Information and Media, 6(2), 2004, 105-111.

Chellappa, R. & Sin, R.G.: Personalization Versus Privacy: An Empirical Examination of the Online Consumer's Dilemma. Information Technology and Management, 6, 2005, 181-202.

Chen, J.V., Ross, W. & Huang, S.F.: Privacy, Trust, and Justice Considerations for Location-Based Mobile Telecommunication Services. info, 10(4), 2008, 30-45.

Chen, J.V. & Ross, W.H.: The Managerial Decision to Implement Electronic Surveillance at Work. International Journal of Organizational Analysis, 13(3), 2005, 244-268.

Clarke, R.: Information Technology and Dataveillance. Communications of the ACM, 31(5), 1988, 498-512.

Clarke, R.: Profiling: A Hidden Challenge to the Regulation of Data Surveillance. 1993, http://www.roger-clarke.com/DV/PaperProfiling.html.

Clarke, R.: The Digital Persona and Its Application to Data Surveillance. 1994, http://www.roger-clarke.com/DV/DigPersona.html.

Clarke, R.: Introduction to Dataveillance and Information Privacy, and Definitions of Terms. 1997, http://www.anu.edu.au/people/Roger.Clarke/DV/Intro.html.

Clarke, R.: Person Location and Person Tracking - Technologies, Risks and Policy Implications. Information Technology & People, 14(2), 2001b, 206-231.

Clarke, R.: Privacy as a Means of Engendering Trust in Cyberspace Commerce. The University of New South Wales Law Journal, 24(1), 2001c, 290-297.

Clarke, R.: While You Were Sleeping… Surveillance Technologies Arrived. Australian Quarterly, 73(1), 2001d, 10-14.

Clarke, R.: Privacy on the Move: The Impacts of Mobile Technologies on Consumers and Citizens. 2003b, http://www.anu.edu.au/people/Roger.Clarke/DV/MPrivacy.html.

Clarke, R.: Have We Learnt to Love Big Brother? Issues, 71, June, 2005, 9-13.

Clarke, R.: What's 'Privacy'? 2006, http://www.rogerclarke.com/DV/Privacy.html.

Clarke, R. Chapter 3. What 'Uberveillance' Is and What to Do About It, in K. Michael and M.G. Michael (eds.), The Second Workshop on the Social Implications of National Security, University of Wollongong, Wollongong, Australia, 2007a, 27-46.

Clarke, R.: Chapter 4. Appendix to What 'Uberveillance' Is and What to Do About It: Surveillance Vignettes, in K. Michael and M.G. Michael (eds.), The Second Workshop on the Social Implications of National Security, University of Wollongong, Wollongong, Australia, 2007b, 47-60.

Clarke, R.: Surveillance Vignettes Presentation. 2007c, http://www.rogerclarke.com/DV/SurvVign-071029.ppt.

Clarke, R.: Privacy Impact Assessment: Its Origins and Development. Computer Law & Security Review, 25(2), 2009, 123-135.

Clarke, R. & Wigan, M.: You Are Where You've Been: The Privacy Implications of Location and Tracking Technologies. 2011, http://www.rogerclarke.com/DV/YAWYB-CWP.html.

Culnan, M.J. & Bies, R.J.: Consumer Privacy: Balancing Economic and Justice Considerations. Journal of Social Issues, 59(2), 2003, 323-342.

Davis, D.W. & Silver, B.D.: Civil Liberties vs. Security: Public Opinion in the Context of the Terrorist Attacks on America. American Journal of Political Science, 48(1), 2004, pp. 28-46.

Dinev, T., Bellotto, M., Hart, P., Colautti, C., Russo, V. & Serra, I.: Internet Users' Privacy Concerns and Attitudes Towards Government Surveillance – an Exploratory Study of Cross-Cultural Differences between Italy and the United States. 18th Bled eConference eIntegration in Action, Bled, Slovenia, 2005, 1-13.

Dobson, J.E. & Fisher, P.F. Geoslavery. IEEE Technology and Society Magazine, 22(1), 2003, 47-52.

Dobson, J.E. & Fisher, P.F. The Panopticon's Changing Geography. Geographical Review, 97(3), 2007, 307-323.

Dwyer, C., Hiltz, S.R. & Passerini, K.: Trust and Privacy Concern within Social Networking Sites: A Comparison of Facebook and Myspace. Proceedings of the Thirteenth Americas Conference on Information Systems, Keystone, Colorado, 2007, 1-12.

Elliot, G. & Phillips, N. Mobile Commerce and Wireless Computing Systems. Pearson Education Limited, Great Britain, 2004.

Ethics Subgroup IoT: Fact sheet- Ethics Subgroup IoT - Version 4.0, European Commission. 2013, 1-21, http://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&cad=rja&uact=8&ved=0CB0QFjAA&url=http%3A%2F%2Fec.europa.eu%2Finformation_society%2Fnewsroom%2Fcf%2Fdae%2Fdocument.cfm%3Fdoc_id%3D1751&ei=5i7RVK-FHczYavKWgPgL&usg=AFQjCNG_VgeaUP_DIJVwSi-PIww3bC9Ug_w

Freescale Semiconductor Inc. and ARM Inc:, Whitepaper: What the Internet of Things (IoT) Needs to Become a Reality. 2014, 1-16, cache.freescale.com/files/32bit/doc/white_paper/INTOTHNGSWP.pdf

Floridi, L.: Information Ethics: On the Philosophical Foundation of Computer Ethics. Ethics and Information Technology, 1, 1999, 37-56.

Foucault, M. Discipline and Punish: The Birth of the Prison. Second Vintage Books Edition May 1995, Vintage Books: A Division of Random House Inc, New York, 1977.

Fusco, S.J., Michael, K., Aloudat, A. & Abbas, R.: Monitoring People Using Location-Based Social Networking and Its Negative Impact on Trust: An Exploratory Contextual Analysis of Five Types of "Friend" Relationships. IEEE Symposium on Technology and Society, Illinois, Chicago, 2011.

Fusco, S.J., Michael, K., Michael, M.G. & Abbas, R.: Exploring the Social Implications of Location Based Social Networking: An Inquiry into the Perceived Positive and Negative Impacts of Using LBSN between Friends. 9th International Conference on Mobile Business, Athens, Greece, IEEE, 2010, 230-237.

Gagnon, M., Jacob, J.D., Guta, A.: Treatment adherence redefined: a critical analysis of technotherapeutics. Nurs Inq. 20(1), 2013, 60-70.

Ganascia, J.G.: The Generalized Sousveillance Society. Social Science Information, 49(3), 2010, 489-507.

Gandy, O.H.: The Panoptic Sort: A Political Economy of Personal Information. Westview, Boulder, Colorado, 1993.

Giaglis, G.M., Kourouthanassis, P. & Tsamakos, A.: Chapter IV. Towards a Classification Framework for Mobile Location-Based Services, in B.E. Mennecke and T.J. Strader (eds.), Mobile Commerce: Technology, Theory and Applications. Idea Group Publishing, Hershey, US, 2003, 67-85.

Gould, J.B.: Playing with Fire: The Civil Liberties Implications of September 11th. Public Administration Review, 62, 2002, 74-79.

Jorns, O. & Quirchmayr, G.: Trust and Privacy in Location-Based Services. Elektrotechnik & Informationstechnik, 127(5), 2010, 151-155.

Junglas, I. & Spitzmüller, C.: A Research Model for Studying Privacy Concerns Pertaining to Location-Based Services. Proceedings of the 38th Hawaii International Conference on System Sciences, 2005, 1-10.

Kaasinen, E.: User Acceptance of Location-Aware Mobile Guides Based on Seven Field Studies. Behaviour & Information Technology, 24(1), 2003, 37-49.

Kaupins, G. & Minch, R.: Legal and Ethical Implications of Employee Location Monitoring. Proceedings of the 38th Hawaii International Conference on System Sciences. 2005, 1-10.

Kim, D.J., Ferrin, D.L. & Rao, H.R.: Trust and Satisfaction, Two Stepping Stones for Successful E-Commerce Relationships: A Longitudinal Exploration. Information Systems Research, 20(2), 2009, 237-257.

King, L.: Information, Society and the Panopticon. The Western Journal of Graduate Research, 10(1), 2001, 40-50.

Kodl, J. & Lokay, M.: Human Identity, Human Identification and Human Security. Proceedings of the Conference on Security and Protection of Information, Idet Brno, Czech Republic, 2001, 129-138.

Kranenburg, R.V. and Bassi, A.: IoT Challenges, Communications in Mobile Computing. 1(9), 2012, 1-5.

Küpper, A. & Treu, G.: Next Generation Location-Based Services: Merging Positioning and Web 2.0., in L.T. Yang, A.B. Waluyo, J. Ma, L. Tan and B. Srinivasan (eds.), Mobile Intelligence. John Wiley & Sons Inc, Hoboken, New Jersey, 2010, 213-236.

Levin, A., Foster, M., West, B., Nicholson, M.J., Hernandez, T. & Cukier, W.: The Next Digital Divide: Online Social Network Privacy. Ryerson University, Ted Rogers School of Management, Privacy and Cyber Crime Institute, 2008, www.ryerson.ca/tedrogersschool/privacy/Ryerson_Privacy_Institute_OSN_Report.pdf.

Lewis, J.D. & Weigert, A.: Trust as a Social Reality. Social Forces, 63(4), 1985, 967-985.

Lyon, D.: The World Wide Web of Surveillance: The Internet and Off-World Power Flows. Information, Communication & Society, 1(1), 1998, 91-105.

Lyon, D.: Surveillance Society: Monitoring Everyday Life. Open University Press, Phildelphia, PA, 2001.

Lyon, D.: Surveillance Studies: An Overview. Polity, Cambridge, 2007.

Macquarie Dictionary.: 'Uberveillance', in S. Butler, Fifth Edition of the Macquarie Dictionary, Australia's National Dictionary. Sydney University, 2009, 1094.

Mann, S.: Sousveillance and Cyborglogs: A 30-Year Empirical Voyage through Ethical, Legal, and Policy Issues. Presence, 14(6), 2005, 625-646.

Mann, S., Nolan, J. & Wellman, B.: Sousveillance: Inventing and Using Wearable Computing Devices for Data Collection in Surveillance Environments. Surveillance & Society, 1(3), 2003, 331-355.

Mathiesen, K.: What is Information Ethics? Computers and Society, 32(8), 2004, 1-11.

Mattern, F. and Floerkemeier, K.: From the Internet of Computers to the Internet of Things, in Sachs, K., Petrov, I. & Guerrero, P. (eds.), From Active Data Management to Event-Based Systems and More. Springer-Verlag Berlin Heidelberg, 2010, 242-259.

Marx, G.T. & Steeves, V.: From the Beginning: Children as Subjects and Agents of Surveillance. Surveillance & Society, 7(3/4), 2010, 192-230.

Mayer, R.C., Davis, J.H. & Schoorman, F.D.: An Integrative Model of Organizational Trust. The Academy of Management Review, 20(3), 1995, 709-734.

McKnight, D.H. & Chervany, N.L.: What Trust Means in E-Commerce Customer Relationships: An Interdisciplinary Conceptual Typology. International Journal of Electronic Commerce, 6(2), 2001, 35-59.

Metzger, M.J.: Privacy, Trust, and Disclosure: Exploring Barriers to Electronic Commerce. Journal of Computer-Mediated Communication, 9(4), 2004.

Michael, K. & Clarke, R.: Location and Tracking of Mobile Devices: Überveillance Stalks the Streets. Computer Law and Security Review, 29(2), 2013, 216-228.

Michael, K., McNamee, A. & Michael, M.G.: The Emerging Ethics of Humancentric GPS Tracking and Monitoring. International Conference on Mobile Business, Copenhagen, Denmark, IEEE Computer Society, 2006a, 1-10.

Michael, K., McNamee, A., Michael, M.G., and Tootell, H.: Location-Based Intelligence – Modeling Behavior in Humans using GPS. IEEE International Symposium on Technology and Society, 2006b.

Michael, K., Stroh, B., Berry, O., Muhlbauer, A. & Nicholls, T.: The Avian Flu Tracker - a Location Service Proof of Concept. Recent Advances in Security Technology, Australian Homeland Security Research Centre, 2006, 1-11.

Michael, K. and Michael, M.G.: Australia and the New Technologies: Towards Evidence Based Policy in Public Administration (1 ed). Wollongong, Australia: University of Wollongong, 2008, Available at: http://works.bepress.com/kmichael/93

Michael, K. & Michael, M.G.: Microchipping People: The Rise of the Electrophorus. Quadrant, 49(3), 2005, 22-33.

Michael, K. and Michael, M.G.: From Dataveillance to Überveillance (Uberveillance) and the Realpolitik of the Transparent Society (1 ed). Wollongong: University of Wollongong, 2007. Available at: http://works.bepress.com/kmichael/51.

Michael, K. & Michael, M.G.: Innovative Automatic Identification and Location-Based Services: From Bar Codes to Chip Implants. IGI Global, Hershey, PA, 2009.

Michael, K. & Michael, M.G.: The Social and Behavioral Implications of Location-Based Services. Journal of Location-Based Services, 5(3/4), 2011, 1-15, http://works.bepress.com/kmichael/246.

Michael, K. & Michael, M.G.: Sousveillance and Point of View Technologies in Law Enforcement: An Overview, in The Sixth Workshop on the Social Implications of National Security: Sousveillance and Point of View Technologies in Law Enforcement, University of Sydney, NSW, Australia, Feb. 2012.

Michael, K., Roussos, G., Huang, G.Q., Gadh, R., Chattopadhyay, A., Prabhu, S. and Chu, P.: Planetary-scale RFID Services in an Age of Uberveillance. Proceedings of the IEEE, 98.9, 2010, 1663-1671.

Michael, M.G. and Michael, K.: National Security: The Social Implications of the Politics of Transparency. Prometheus, 24(4), 2006, 359-364.

Michael, M.G. & Michael, K. Towards a State of Uberveillance. IEEE Technology and Society Magazine, 29(2), 2010, 9-16.

Michael, M.G. & Michael, K. (eds): Uberveillance and the Social Implications of Microchip Implants: Emerging Technologies. Hershey, PA, IGI Global, 2013.

O'Connor, P.J. & Godar, S.H.: Chapter XIII. We Know Where You Are: The Ethics of LBS Advertising, in B.E. Mennecke and T.J. Strader (eds.), Mobile Commerce: Technology, Theory and Applications, Idea Group Publishing, Hershey, US, 2003, 245-261.

Orwell, G.: Nineteen Eighty Four. McPherson Printing Group, Maryborough, Victoria, 1949.

Oxford Dictionary: Control, Oxford University Press, 2012a http://oxforddictionaries.com/definition/control?q=control.

Oxford Dictionary: Trust, Oxford University Press, 2012b, http://oxforddictionaries.com/definition/trust?q=trust.

Pavlou, P.A.: Consumer Acceptance of Electronic Commerce: Integrating Trust and Risk with the Technology Acceptance Model. International Journal of Electronic Commerce, 7(3), 2003, 69-103.

Perusco, L. & Michael, K.: Humancentric Applications of Precise Location Based Services, in IEEE International Conference on e-Business Engineering, Beijing, China, IEEE Computer Society, 2005, 409-418.

Perusco, L. & Michael, K.: Control, Trust, Privacy, and Security: Evaluating Location-Based Services. IEEE Technology and Society Magazine, 26(1), 2007, 4-16.

Perusco, L., Michael, K. & Michael, M.G.: Location-Based Services and the Privacy-Security Dichotomy, in Proceedings of the Third International Conference on Mobile Computing and Ubiquitous Networking, London, UK, Information Processing Society of Japan, 2006, 91-98.

Quinn, M.J.: Ethics for the Information Age. Second Edition, Pearson/Addison-Wesley, Boston, 2006.

Renegar, B., Michael, K. & Michael, M.G.: Privacy, Value and Control Issues in Four Mobile Business Applications, in 7th International Conference on Mobile Business (ICMB2008), Barcelona, Spain, IEEE Computer Society, 2008, 30-40.

Rozenfeld, M.: The Value of Privacy: Safeguarding your information in the age of the Internet of Everything, The Institute: the IEEE News Source, 2014, http://theinstitute.ieee.org/technology-focus/technology-topic/the-value-of-privacy.

Rummel, R.J.: Death by Government. Transaction Publishers, New Brunswick, New Jersey, 1997.

Sanquist, T.F., Mahy, H. & Morris, F.: An Exploratory Risk Perception Study of Attitudes toward Homeland Security Systems. Risk Analysis, 28(4), 2008, 1125-1133.

Schoorman, F.D., Mayer, R.C. & Davis, J.H.: An Integrative Model of Organizational Trust: Past, Present, and Future. Academy of Management Review, 32(2), 2007, 344-354.

Shay, L.A., Conti, G., Larkin, D., Nelson, J.: A framework for analysis of quotidian exposure in an instrumented world. IEEE International Carnahan Conference on Security Technology (ICCST), 2012, 126-134.

Siau, K. & Shen, Z.: Building Customer Trust in Mobile Commerce. Communications of the ACM, 46(4), 2003, 91-94.

Solove, D.: Digital Dossiers and the Dissipation of Fourth Amendment Privacy. Southern California Law Review, 75, 2002, 1083-1168.

Solove, D.: The Digital Person: Technology and Privacy in the Information Age. New York University Press, New York, 2004.

Tavani, H.T.: Ethics and Technology: Ethical Issues in an Age of Information and Communication Technology. John Wiley, Hoboken, N.J., 2007.

Valacich, J.S.: Ubiquitous Trust: Evolving Trust into Ubiquitous Computing Environments. Business, Washington State University, 2003, 1-2.

van Ooijen, C. & Nouwt, S.: Power and Privacy: The Use of LBS in Dutch Public Administration, in B. van Loenen, J.W.J. Besemer and J.A. Zevenbergen (eds.), Sdi Convergence. Research, Emerging Trends, and Critical Assessment, Nederlandse Commissie voor Geodesie Netherlands Geodetic Commission 48, 2009, 75-88.

Wakunuma, K.J. and Stahl, B.C.: Tomorrow's Ethics and Today's Response: An Investigation into The Ways Information Systems Professionals Perceive and Address Emerging Ethical Issues. Inf Syst Front, 16, 2014, 383–397.

Weckert, J.: Trust and Monitoring in the Workplace. IEEE International Symposium on Technology and Society, 2000. University as a Bridge from Technology to Society, 2000, 245-250.

Wigan, M. & Clarke, R.: Social Impacts of Transport Surveillance. Prometheus, 24(4), 2006, 389-403.

Xu, H. & Teo, H.H.: Alleviating Consumers' Privacy Concerns in Location-Based Services: A Psychological Control Perspective. Twenty-Fifth International Conference on Information Systems, 2004, 793-806.

Xu, H., Teo, H.H. & Tan, B.C.Y.: Predicting the Adoption of Location-Based Services: The Role of Trust and Perceived Privacy Risk. Twenty-Sixth International Conference on Information Systems, 2005, 897-910.

Yan, Z. & Holtmanns, S.: Trust Modeling and Management: From Social Trust to Digital Trust, in R. Subramanian (ed.), Computer Security, Privacy and Politics: Current Issues, Challenges and Solutions. IGI Global, 2008, 290-323.

Yeh, Y.S. & Li, Y.M.: Building Trust in M-Commerce: Contributions from Quality and Satisfaction. Online Information Review, 33(6), 2009, 1066-1086.

Sandrina Dimitrijevic:

Ethical Consequences of Bounded Rationality in the Internet of Things

Abstract:

One of the main challenges that the arriving paradigm of Internet of Things brings to society is providing and securing individual privacy. There are lots of obstacles which prevents us from successfully confronting such a challenge. In this paper we are going to deal with one such obstacle, and that is the bounded rationality of humans as participants in the environment of Internet of Things. We argue that the ethical approach to the vision of the Internet of Things has to include the notion of bounded rationality. Bounded rationality of users impedes the possibility of giving informed consent. Informed consent is required when getting permission for collecting and using somebody's personal information. Lastly, we discuss the need for a paternalistic approach of maximum possible default privacy settings without asking for consent, given the seriousness of all potential risks.

Agenda:

Author:

MSc: Sandrina Dimitrijevic

- PhD candidate at the Faculty of Economics, Belgrade University
- anirdnas@gmail.com

ISSN 1614-1687

Development of information technologies is proceeding very fast, and one of the expected steps in such process is the arrival of Internet of Things. Internet of Things presents a scenario where multiple things we are surrounded with can communicate between each other, without people being aware of it. Such scenario has multiple possible benefits, but brings with itself a lot of challenges as well. The most important and critical challenge is the endangerment of personal privacy. The pervasive interconnectedness of smart objects makes privacy concerns larger than ever. In the paradigm of Internet of Things risks will be distributed much more widely compared to the present situation[1]. Some of the dark scenarios of new technologies include possibility of surveillance in real time or disappearance of the difference between public and private space[2].

For such reasons, proactive approach to design and implementations of such technologies is needed. Ethical issues should be evaluated carefully. Solving the challenges of new technologies will undoubtedly involve new ethical rules, standards and ways of behaviour, much different than the one which already exist in offline environment[3].

How can privacy be jeopardized in the Internet of Things?

Right to privacy has been recognised as one of the most essential human rights in society. It helps nurture democratic societies, ensures human dignity and freedom of speech and choice.

Information and communication technologies make things people perform every day far easier, and bridge the gap of space and time. Internet of Things is being made with the purpose of bringing greater benefit to human kind[4].

However, its longer term success might depend on how successfully the issue of privacy concerns is addressed[5]. Threat to privacy doesn't come as a pre-planned intention, but is a result of inherent characteristics present in new technologies. However, there are views saying that technologies of smart things and ubiquitous computing are violent, pervasive and can turn things into surveillance objects[6].

People might become hesitant in accepting such technologies, if they feel their privacy is threatened[7]. Couple of main sources of privacy risk are being distinguished in the environment of the Internet of Things.

An unprecedented level of data sharing

The vision of Internet of Things includes a notion of smart objects which will be present everywhere. They could include things in our pockets or be integrated into our home and work environment. Sensors might exist in many physical objects people regularly pass by. As the number of smart objects increases, the amount of

1 Atzori, Luigi, Antonio Iera, and Giacomo Morabito. "The internet of things: A survey." Computer networks 54.15 (2010): 2787-2805.

2 De Hert, Paul, et al. "Legal safeguards for privacy and data protection in ambient intelligence." Personal and ubiquitous computing 13.6 (2009): 435-444.

3 Maner, Walter. "Unique ethical problems in information technology." Science and Engineering Ethics 2.2 (1996): 137-154.

4Atzori, Luigi, Antonio Iera, and Giacomo Morabito. "The internet of things: A survey." Computer networks 54.15 (2010): 2787-2805.

5 Hong, Jason I., et al. "Privacy risk models for designing privacy-sensitive ubiquitous computing systems." Proceedings of the 5th conference on Designing interactive systems: processes, practices, methods, and techniques. ACM, 2004.

6 Araya, Agustin A. "Questioning ubiquitous computing." Proceedings of the 1995 ACM 23rd annual conference on Computer science. ACM, 1995.

7 Atzori, Luigi, Antonio Iera, and Giacomo Morabito. "The internet of things: A survey." Computer networks 54.15 (2010): 2787-2805.

ISSN 1614-1687

data being stored, shared and mined will keep rising like never before. Consequently, there will be a lot more opportunities for data to be compromised[8].

Data Mining and Profiling

The presence of tremendous and constantly increasing amount of data brings new risks, even if such data is completely anonymized. Publicly available and unprotected data can be mined and analysed through the use of special algorithms revealing patterns and sensitive personal information. For example, it has been shown that mining data about energy consumption can expose in-home activities, like sleep cycles, usage of appliances and more, which can be abused by criminals or marketers[9]. It doesn't even help if such data is anonymized because de-anonymizing techniques can be used to re-identify people[10].

Big Data and Analytics

The previously unimaginable amount of data is recognized as a great business opportunity[11]. Businesses and companies can use all available data to make better strategic decisions and further adjust their products and services toward customer needs. Such activities not only help improve profits and growth, but are beneficial for the customers as well. For example, data can be used to provide customers with recommendations which increase their overall contentment[12] or provide them with a more valuable personalized experience[13]. On the other side, it has already been remarked that such practices convey significant legal and ethical problems[14].

Unauthorized Access/Security

Data security is one more urgent issue which causes worries. As physical objects integrated into Internet of Things are often left unattended, and as their number increases the likelihood of unauthorized use is also growing[15]. Eavesdropping is easier in wireless communications. Communication between different objects might be intercepted and altered for unethical use[16]. Moreover, such data is likely to be standardized, as that is necessary for deriving the highest possible benefits of Internet of Things. Such standards are still being developed, but it can be argued that standardization imposes greater risk to security, as standardized data is easier to capture.

---

8 Vermesan, Ovidiu, et al. "Internet of things strategic research roadmap."Internet of Things-Global Technological and Societal Trends (2011): 9-52.

9 Lisovich, Mikhail A., Deirdre K. Mulligan, and Stephen B. Wicker. "Inferring personal information from demand-response systems." Security & Privacy, IEEE 8.1 (2010): 11-20.

10 Narayanan, Arvind, and Vitaly Shmatikov. "De-anonymizing social networks."Security and Privacy, 2009 30th IEEE Symposium on. IEEE, 2009.

11 Chen, Hsinchun, Roger HL Chiang, and Veda C. Storey. "Business Intelligence and Analytics: From Big Data to Big Impact." MIS quarterly 36.4 (2012): 1165-1188.

12 Ricci, Francesco, Lior Rokach, and Bracha Shapira. Introduction to recommender systems handbook. Springer US, 2011.

13 Eirinaki, Magdalini, and Michalis Vazirgiannis. "Web mining for web personalization." ACM Transactions on Internet Technology (TOIT) 3.1 (2003): 1-27.

14 Caudill, Eve M., and Patrick E. Murphy. "Consumer online privacy: legal and ethical issues." Journal of Public Policy & Marketing 19.1 (2000): 7-19.

15 Atzori, Luigi, Antonio Iera, and Giacomo Morabito. "The internet of things: A survey." Computer networks 54.15 (2010): 2787-2805.

16 Atzori, Luigi, Antonio Iera, and Giacomo Morabito. "The internet of things: A survey." Computer networks 54.15 (2010): 2787-2805.

Technological Uncertainty

The cost of storing data keeps decreasing which means that such data might be stored somewhere on servers for indefinite time[17]. That carries further challenges as ttechnologies constantly keep changing. It is hard to predict what comes next and for that reason, there is a certain level of uncertainty in dealing with data. The current level of protection might make all data on server safe, but next year new procedures might be developed, which would manage to break the current security protection. When companies get approval for using data for a specified purpose, it would be hard to maintain the promise in the presence of high uncertainty.

Bounded rationality as an obstacle for informed consent

In dealing with privacy of data shared with different services, it is often assumed that the ethical approach involves letting users know what data is being collected by the service and asking them to agree on that[18]. If users are not fully informed about such practices they simply need to be educated and ways of opting out from data collection procedures should be provided[19]. Similar scenario is being suggested for the use of RFID tags in smart objects. Users could specify their own privacy policies for all RFID tags, choose how to use them, disable or send them into the sleep mode[2021].

However, such practices might be shown to be ineffective as it has been found that when making privacy related decisions people are not behaving rationally, as it is often assumed[22]. People report being concerned about their privacy, but keep behaving completely opposite[23]. Furthermore, some research has shown that user decisions of whether to share their data or not is highly sensitive to how question itself is framed[24].

Such behavior can be explained by the notion of bounded rationality. Concept of bounded rationality has been popularized and empirically investigated with the rise of behavioral economics, and it encompasses the notion that individuals are limited when making decisions by their computational power, cognitive bias, information and time[2526]. Some authors have already argued that it might be the cause of unethical behavior in general decision making[27].

The importance of the concept of bounded rationality lies in the fact that it prevents informed consent, which is extremely important in ethical practices. Not only from a legal point of view, but also from ethical and moral one as well, it is a necessary condition to be fulfilled in situation when users are being asked to share their data

17 Atzori, Luigi, Antonio Iera, and Giacomo Morabito. "The internet of things: A survey." Computer networks 54.15 (2010): 2787-2805.

18 Milne, George R. "Privacy and ethical issues in database/interactive marketing and public policy: a research framework and overview of the special issue."Journal of Public Policy & Marketing 19.1 (2000): 1-6.

19 Nowak, Glen J., and Joseph Phelps. "Understanding privacy concerns. An assessment of consumers' information-related knowledge and beliefs." Journal of Direct Marketing 6.4 (1992): 28-39.

20 Molnar, David, Andrea Soppera, and David Wagner. "Privacy for RFID through trusted computing." Proceedings of the 2005 ACM workshop on Privacy in the electronic society. ACM, 2005.

21 Juels, Ari. "RFID security and privacy: A research survey." Selected Areas in Communications, IEEE Journal on 24.2 (2006): 381-394.

22 Acquisti, Alessandro, and Jens Grossklags. "Privacy and rationality in individual decision making." IEEE Security & Privacy 2 (2005): 24-30.

23 Berendt, Bettina, Oliver Günther, and Sarah Spiekermann. "Privacy in e-commerce: stated preferences vs. actual behavior." Communications of the ACM 48.4 (2005): 101-106.

24 Bellman, Steven, Eric J. Johnson, and Gerald L. Lohse. "On site: to opt-in or opt-out?: it depends on the question." Communications of the ACM 44.2 (2001): 25-27.

25 Simon, Herbert Alexander. Models of bounded rationality: Empirically grounded economic reason. Vol. 3. MIT press, 1982.

26 Kahneman, Daniel. "Maps of bounded rationality: Psychology for behavioral economics." American economic review (2003): 1449-1475.

27 Palazzo, Guido, Franciska Krings, and Ulrich Hoffrage. "Ethical blindness." Journal of business ethics 109.3 (2012): 323-338.

with services and companies. If informed consent cannot be guaranteed, that undoubtedly creates an urgent ethical dilemma because such data can be misused with significant negative consequences for the individual and even the whole society. For attaining informed consent one needs to fulfill criteria of full disclosure, comprehension, competence, voluntarity and agreement[28]. That is not always the case in digital environment and indeed, the existence of informed consent for users of privacy-challenging technologies has already been challenged[29].

What are the main observed characteristics of human psyche which prevent users from behaving rationally?

Cognitive and Time Limits

From the point of common sense, it is simply reasonable to assume that users won't have enough time to read and contemplate on all available privacy policies and practices. Such behaviour is already observed in the context of internet privacy policies, as large number of users simply do not read them[30]. In the environment of Internet of Things, each of the smart things could have its own privacy policy or terms of use, but expecting that each of them will be thoroughly analysed before acceptance of use is unrealistic. Moreover, privacy policies can contain legal jargon, which is simply hard to understand[31]. Additionally, ordinary internet users are reported to have problems understanding common computer and Internet terms, their own behaviour or valuations[32]. As the concept of Internet of Things is even more complex such misunderstandings could only be more emphasized in the future. The percentage of users who would have troubles understanding what smart objects are doing and how can data be shared will without a doubt be significantly higher.

Hyperbolic Discounting and Self-Control

Even privacy concerned individuals are found to share their data for negligible benefit[33]. Human decision making is often automatic, and when individuals are faces with a trade-off of choosing between short term conveniences versus costs of reduced privacy in long term, they choose the convenience[34]. Such behaviour could be explained with a phenomenon of hyperbolic discounting, when individuals put a very low value on future reduced privacy costs at the current moment, but change that evaluation in the future[35]. It is also closely connected with the problem of self-control and impulsive behaviour which are well-known features of human psyche[36]. Given that human privacy preferences are not stable and time consistent, such behaviour might be problematic for service designer, because even if users have now accepted data sharing with smart things,

28 Millett, Lynette I., Batya Friedman, and Edward Felten. "Cookies and web browser design: toward realizing informed consent online." Proceedings of the SIGCHI conference on Human factors in computing systems. ACM, 2001.

29 Jensen, Carlos, Colin Potts, and Christian Jensen. "Privacy practices of Internet users: self-reports versus observed behavior." International Journal of Human-Computer Studies 63.1 (2005): 203-227.

30 Jensen, Carlos, Colin Potts, and Christian Jensen. "Privacy practices of Internet users: self-reports versus observed behavior." International Journal of Human-Computer Studies 63.1 (2005): 203-227.

31 Pollach, Irene. "A typology of communicative strategies in online privacy policies: Ethics, power and informed consent." Journal of Business Ethics 62.3 (2005): 221-235.

32 Jensen, Carlos, Colin Potts, and Christian Jensen. "Privacy practices of Internet users: self-reports versus observed behavior." International Journal of Human-Computer Studies 63.1 (2005): 203-227.

33 Spiekermann, Sarah, Jens Grossklags, and Bettina Berendt. "E-privacy in 2nd generation E-commerce: privacy preferences versus actual behavior." Proceedings of the 3rd ACM conference on Electronic Commerce. ACM, 2001.

34 Acquisti, Alessandro. "Privacy in electronic commerce and the economics of immediate gratification." Proceedings of the 5th ACM conference on Electronic commerce. ACM, 2004.

35 Acquisti, Alessandro, and Jens Grossklags. "Losses, gains, and hyperbolic discounting: An experimental approach to information security attitudes and behavior." 2nd Annual Workshop on Economics and Information Security-WEIS. Vol. 3. 2003.

36 Baumeister, Roy F. "Yielding to temptation: Self-control failure, impulsive purchasing, and consumer behavior." Journal of Consumer Research 28.4 (2002): 670-676.

they can easily change their mind as time passes. Given that possible privacy risks are far greater in Internet of Things, we could argue that such future privacy costs might be even higher; causing outcry by users who have previously accepted such costs in exchange for short term convenience.

Status Quo Bias

Status quo bias describes the human propensity to prefer the current state of the things. Such cognitive bias affects decision in adjusting software or services default settings. Each piece of software or a service usually comes with a set of predefined settings, which are rarely being changed, even if they interfere with stated user preference[37]. Same is valid for privacy settings, which are seldom being changed[38]. Humans simply prefer the status quo situation.

Illusion of Control

An additional paradoxical phenomenon which has been observed in the context of privacy protection techniques is the control paradox. It explains type of behaviour when a mere feeling that individuals have control over publication of their data, makes them more inclined to disclose personal data, increasing the overall objective risk[39].

Proposed solutions

Future scenario of the Internet of Things involves a vision of intelligent and smart objects and surfaces which can communicate in the background completely unnoticeably. At the same time, we have shown human beings are rationally bounded and unable to fully contemplate or control what is happening. Such a combination can have multiple unforeseen and dangerous consequences. Moral goals need to consider the complete nature of human beings[40].

The need for addressing this challenge is even more emphasized if we have in mind that information technology's designers themselves aren't interested in ethical consequences of their technologies[41]. Usually, the ethical worries appear as an ex-post problem. And even in such situations, as service designers are humans themselves, they might fail to view the ethical challenge or can find excuses for it[42]. Organizational structure can also hinder ethicality[43].

The discussion of dealing with the problem of privacy in the surrounding of humans and increasingly smarter things is ongoing. Currently proposed approaches of better authentication or encryption or increasing the

37 Smith, N. Craig, Daniel G. Goldstein, and Eric J. Johnson. "Choice without awareness: ethical and policy implications of defaults." Journal of Public Policy & Marketing 32.2 (2013): 159-172.

38 Gross, Ralph, and Alessandro Acquisti. "Information revelation and privacy in online social networks." Proceedings of the 2005 ACM workshop on Privacy in the electronic society. ACM, 2005.

39 Brandimarte, Laura, Alessandro Acquisti, and George Loewenstein. "Misplaced confidences privacy and the control paradox." Social Psychological and Personality Science 4.3 (2013): 340-347.

40 Gigerenzer, Gerd. "Moral satisficing: Rethinking moral behavior as bounded rationality." Topics in cognitive science 2.3 (2010): 528-554.

41 Wakunuma, Kutoma J., and Bernd Carsten Stahl. "Tomorrow's ethics and today's response: An investigation into the ways information systems professionals perceive and address emerging ethical issues." Information Systems Frontiers (2014): 1-15.

42 Tenbrunsel, Ann E., and David M. Messick. "Ethical fading: The role of self-deception in unethical behavior." Social Justice Research 17.2 (2004): 223-236.

43 Kish-Gephart, Jennifer J., David A. Harrison, and Linda Klebe Treviño. "Bad apples, bad cases, and bad barrels: meta-analytic evidence about sources of unethical decisions at work." Journal of Applied Psychology 95.1 (2010): 1.

amount of control of users over their data[44] are not enough. There are also approaches suggesting the use of having privacy assistants directly incorporated into the software, which will warn users every time they are sharing sensitive information[45].

One potentially promising approach to addressing privacy concerns is the concept of privacy by design. Privacy by design is a term coined by Ann Chavoukin, Canadian privacy expert in 1997[46]. It encompasses a notion that all technologies with privacy-intrusive potential are required to provide maximum possible privacy settings by default, and such principle has to be respected from the first day of software design. Privacy by design principles could be especially important in the environment of ubiquitous computing, given its pervasivity and gravity of possible consequences[47]. We can argue that it would basically involve a paternalistic approach, which would mean the maximum achievable benefit for users, without asking for their approval. Paternalism has already been suggested as a solution for dealing with privacy-invasive technologies[48].

However, it is highly probable that companies will hesitate to implement such principles into their own systems, for the reason of high cost and loss of profit. In such case adequate legislation is needed[49], maybe even on international level[50].

References

Ackerman, Mark S., and Lorrie Cranor. "Privacy critics: UI components to safeguard users' privacy." CHI'99 Extended Abstracts on Human Factors in Computing Systems. ACM, 1999.

Acquisti, Alessandro, and Jens Grossklags. "Losses, gains, and hyperbolic discounting: An experimental approach to information security attitudes and behavior." 2nd Annual Workshop on Economics and Information Security-WEIS. Vol. 3. 2003.

Acquisti, Alessandro, and Jens Grossklags. "Privacy and rationality in individual decision making." IEEE Security & Privacy 2 (2005): 24-30.

Acquisti, Alessandro. "Privacy in electronic commerce and the economics of immediate gratification." Proceedings of the 5th ACM conference on Electronic commerce. ACM, 2004.

Araya, Agustin A. "Questioning ubiquitous computing." Proceedings of the 1995 ACM 23rd annual conference on Computer science. ACM, 1995.

Atzori, Luigi, Antonio Iera, and Giacomo Morabito. "The internet of things: A survey." Computer networks 54.15 (2010): 2787-2805.

Baumeister, Roy F. "Yielding to temptation: Self-control failure, impulsive purchasing, and consumer behavior." Journal of Consumer Research 28.4 (2002): 670-676.

Bellman, Steven, Eric J. Johnson, and Gerald L. Lohse. "On site: to opt-in or opt-out?: it depends on the question." Communications of the ACM 44.2 (2001): 25-27.

Berendt, Bettina, Oliver Günther, and Sarah Spiekermann. "Privacy in e-commerce: stated preferences vs. actual behavior." Communications of the ACM 48.4 (2005): 101-106.

44 Atzori, Luigi, Antonio Iera, and Giacomo Morabito. "The internet of things: A survey." Computer networks 54.15 (2010): 2787-2805.

45 Ackerman, Mark S., and Lorrie Cranor. "Privacy critics: UI components to safeguard users' privacy." CHI'99 Extended Abstracts on Human Factors in Computing Systems. ACM, 1999.

46 Cavoukian, Ann. "Privacy by design." Take the Challenge. Information and Privacy Commissioner of Ontario, Canada (2009).

47 Langheinrich, Marc. "Privacy by design—principles of privacy-aware ubiquitous systems." Ubicomp 2001: Ubiquitous Computing. Springer Berlin Heidelberg, 2001.

48 Smith, N. Craig, Daniel G. Goldstein, and Eric J. Johnson. "Choice without awareness: ethical and policy implications of defaults." Journal of Public Policy & Marketing 32.2 (2013): 159-172.

49 Langheinrich, Marc. "A survey of RFID privacy approaches." Personal and Ubiquitous Computing 13.6 (2009): 413-421.

50 Weber, Rolf H. "Internet of Things–New security and privacy challenges."Computer Law & Security Review 26.1 (2010): 23-30.

Brandimarte, Laura, Alessandro Acquisti, and George Loewenstein. "Misplaced confidences privacy and the control paradox." Social Psychological and Personality Science 4.3 (2013): 340-347.

Caudill, Eve M., and Patrick E. Murphy. "Consumer online privacy: legal and ethical issues." Journal of Public Policy & Marketing 19.1 (2000): 7-19.

Cavoukian, Ann. "Privacy by design." Take the Challenge. Information and Privacy Commissioner of Ontario, Canada (2009).

Chen, Hsinchun, Roger HL Chiang, and Veda C. Storey. "Business Intelligence and Analytics: From Big Data to Big Impact." MIS quarterly 36.4 (2012): 1165-1188.

De Hert, Paul, et al. "Legal safeguards for privacy and data protection in ambient intelligence." Personal and ubiquitous computing 13.6 (2009): 435-444.

Eirinaki, Magdalini, and Michalis Vazirgiannis. "Web mining for web personalization." ACM Transactions on Internet Technology (TOIT) 3.1 (2003): 1-27.

Gigerenzer, Gerd. "Moral satisficing: Rethinking moral behavior as bounded rationality." Topics in cognitive science 2.3 (2010): 528-554.

Gross, Ralph, and Alessandro Acquisti. "Information revelation and privacy in online social networks." Proceedings of the 2005 ACM workshop on Privacy in the electronic society. ACM, 2005.

Hong, Jason I., et al. "Privacy risk models for designing privacy-sensitive ubiquitous computing systems." Proceedings of the 5th conference on Designing interactive systems: processes, practices, methods, and techniques. ACM, 2004.

Jensen, Carlos, Colin Potts, and Christian Jensen. "Privacy practices of Internet users: self-reports versus observed behavior." International Journal of Human-Computer Studies 63.1 (2005): 203-227.

Juels, Ari. "RFID security and privacy: A research survey." Selected Areas in Communications, IEEE Journal on 24.2 (2006): 381-394.

Kahneman, Daniel. "Maps of bounded rationality: Psychology for behavioral economics." American economic review (2003): 1449-1475.

Kish-Gephart, Jennifer J., David A. Harrison, and Linda Klebe Treviño. "Bad apples, bad cases, and bad barrels: meta-analytic evidence about sources of unethical decisions at work." Journal of Applied Psychology 95.1 (2010): 1.

Langheinrich, Marc. "A survey of RFID privacy approaches." Personal and Ubiquitous Computing 13.6 (2009): 413-421.

Langheinrich, Marc. "Privacy by design—principles of privacy-aware ubiquitous systems." Ubicomp 2001: Ubiquitous Computing. Springer Berlin Heidelberg, 2001.

Lisovich, Mikhail A., Deirdre K. Mulligan, and Stephen B. Wicker. "Inferring personal information from demand-response systems." Security & Privacy, IEEE 8.1 (2010): 11-20.

Maner, Walter. "Unique ethical problems in information technology." Science and Engineering Ethics 2.2 (1996): 137-154.

Millett, Lynette I., Batya Friedman, and Edward Felten. "Cookies and web browser design: toward realizing informed consent online." Proceedings of the SIGCHI conference on Human factors in computing systems. ACM, 2001.

Milne, George R. "Privacy and ethical issues in database/interactive marketing and public policy: a research framework and overview of the special issue."Journal of Public Policy & Marketing 19.1 (2000): 1-6.

Molnar, David, Andrea Soppera, and David Wagner. "Privacy for RFID through trusted computing." Proceedings of the 2005 ACM workshop on Privacy in the electronic society. ACM, 2005.

Narayanan, Arvind, and Vitaly Shmatikov. "De-anonymizing social networks."Security and Privacy, 2009 30th IEEE Symposium on. IEEE, 2009.

Nowak, Glen J., and Joseph Phelps. "Understanding privacy concerns. An assessment of consumers' information-related knowledge and beliefs." Journal of Direct Marketing 6.4 (1992): 28-39.

Palazzo, Guido, Franciska Krings, and Ulrich Hoffrage. "Ethical blindness." Journal of business ethics 109.3 (2012): 323-338.

Pollach, Irene. "A typology of communicative strategies in online privacy policies: Ethics, power and informed consent." Journal of Business Ethics 62.3 (2005): 221-235.

Ricci, Francesco, Lior Rokach, and Bracha Shapira. Introduction to recommender systems handbook. Springer US, 2011.

Simon, Herbert Alexander. Models of bounded rationality: Empirically grounded economic reason. Vol. 3. MIT press, 1982.

Smith, N. Craig, Daniel G. Goldstein, and Eric J. Johnson. "Choice without awareness: ethical and policy implications of defaults." Journal of Public Policy & Marketing 32.2 (2013): 159-172.

Spiekermann, Sarah, Jens Grossklags, and Bettina Berendt. "E-privacy in 2nd generation E-commerce: privacy preferences versus actual behavior." Proceedings of the 3rd ACM conference on Electronic Commerce. ACM, 2001.

Tenbrunsel, Ann E., and David M. Messick. "Ethical fading: The role of self-deception in unethical behavior." Social Justice Research 17.2 (2004): 223-236.

Vermesan, Ovidiu, et al. "Internet of things strategic research roadmap."Internet of Things-Global Technological and Societal Trends (2011): 9-52.

Wakunuma, Kutoma J., and Bernd Carsten Stahl. "Tomorrow's ethics and today's response: An investigation into the ways information systems professionals perceive and address emerging ethical issues." Information Systems Frontiers (2014): 1-15.

Weber, Rolf H. "Internet of Things–New security and privacy challenges. "Computer Law & Security Review 26.1 (2010): 23-30.

Kashif Habib:

Ethical Aspects of the Internet of Things in eHealth

Abstract:

While the current Internet has brought comforts in our lives, the future of the Internet that is the Internet of Things (IoT) promises to make our daily living even much easier and convenient. The IoT presents a concept of smart world around us, where things are trying to assist and benefit people. Patient monitoring outside the hospital environment is one case for the IoT in healthcare. The healthcare system can get many benefits from the IoT such as patient monitoring with chronic disease, monitoring of elderly people, and monitoring of athletes fitness. However, the comfort may bring along some worries in the form of people's concerns such as right or wrong actions by things, unauthorised tracking, illegal monitoring, trust relationship, safety, and security. This paper presents the ethical implications of the IoT in eHealth on people and society, and more specifically discusses the ethical issues that may arise due to distinguishing characteristics of the IoT.

Agenda:

Author:

Kashif Habib

- Norsk Regnesentral/Norwegian Computing Center,
  P.O. Box 114 Blindern, NO-0314 Oslo, Norway
- ☎ + 47 - 22 85 25 00 , ✉ Kashif.Sheikh@nr.no, 💻 www.nr.no

Acknowledgment

The work presented here has been carried out in the research project ASSET – Adaptive Security for Smart Internet of Things in eHealth (2012–2015) funded by The Research Council of Norway. The author would like to thank Sven Arntzen, Arild Torjusen, and Wolfgang Leister for their comments and for helpful discussions.

ISSN 1614-1687

Introduction

The IoT envisions merging the physical world with the digital world. The IoT provides new ways of communication between people and things and between things themselves. According to CISCO systems, the IoT combines data, people, processes, and things together to enrich the networked connectivity[1]. The IoT is a network of interconnected things such as sensors, Near Field Communication (NFC) tags, Radio Frequency Identification (RFID) tags, actuators, smartphones, tablets, computers, etc. In the IoT, all kind of things will exchange information[2], work in synergy[3], and embed real world information into networks[4]. Communication and the capability to perceive information from surroundings can provide many benefits to domains like transportation, healthcare, personal, social, home, office and industry[5].

In this article, we highlight the ethical implications of the IoT in eHealth on people and society, and more specifically discusses the ethical issues that may arise due to distinguishing characteristics of the IoT.

IoT in eHealth

Patient monitoring outside the hospital environment is one case for the IoT in healthcare[6]. While monitoring patient's health parameters with on-body sensors, the IoT may allow a patient to be at different locations such as home, office, public place, or in a vehicle but medical sensors still connected and transmitting information to the doctor's office. The healthcare system can get many benefits from the IoT, such as patient monitoring with chronic disease, monitoring of elderly people, monitoring of athletes fitness, and in terms of getting quick medical response from the medical practitioner while suffering from intense condition.

The main objective of the IoT in eHealth system is to assist the existing healthcare system by monitoring the vital signs of patient's health data in real time. From systems point of view, complete and accurate information transfer from a patient to the medical centre is always necessary. Failure to do so may cause a threat to the patient's life. Also, other people with bad intentions can send wrong data to the hospital by miss utilising the devices. Transferring a patient's health data to a remote medical centre opens for security threats that may impact the patient's privacy and trust, confidentiality of data transmission, integrity of received data, and data availability. Patient's privacy and trust are certainly the important challenges in the deployment of patient monitoring system. Although, trust can be defined[7] for different purposes and application areas in several disciplines, one way of defining trust in the eHealth system is simple. If the patient monitoring system can ensure that the patient's data is used and accessible by only authorised users and system interruption may not endanger patient's life or lead into wrong treatment, then it may serve the purpose. Protection, safety, privacy, and trust establishment in the IoT in eHealth is a major challenge due to the dynamic and complex nature of the system. In such systems, safety and privacy requirements are affected by the changes in the internal and external conditions of the system.

1 Evans, D.: Internet of Everything (IoE), CISCO Blogs, (2013), http://blogs.cisco.com/ioe/.

2 Sundmaeker, H., Guillemin, P., Friess, P., and Woelfflé, S.:Vision and challenges for realising the Internet of Things, Cluster of European Research Projects on the Internet of Things—CERP IoT, (2010) 1-236.

3 Future Internet Strategic Research Agenda, Version 1.1, European Future Internet X-ETP Group, (2010) 1-73.

4 Vermesan, O. et al.: Internet of Things Strategic Research Roadmap 2011, European Research Cluster on the Internet of Things, (2011) 1-44.

5 Atzoria, L., Ierab, A., Morabito, G.: The Internet of Things, A survey, Computer Networks (54), (2010) 2787-2805.

6 Habib,K., Torjusen,A., and Leister, W.: A Novel Authentication Framework Based on Biometric and Radio Fingerprinting for the IoT in eHealth,(2014) 32-37.

7 Leister,W., and Schulz, T.:Ideas for a trust indicator in the Internet of Things, (2012), 31-34.

ISSN 1614-1687

Ethical Issues

With the passage of time, science and technology have a greater impact and influence on human lives that seems a strong case in the IoT as well. Ethics can be considered to be the systematic theory about moral principles, values and codes. The word ethics comes from the Greek word ethos that can mean beliefs, customs, and character. It is very often interchangeably used with the term morals, beliefs or principles as well. At the same time, when we hear the word ethics automatically we think about rules that would distinguish right from wrong. The ethical theories can be considered as guidelines for people to behave rationally and according to moral values. The ethical theories can help us in many ways, such as understanding of right versus wrong, acknowledging moral values, our moral responsibilities, awareness of our own actions, and who and how people can be affected by our actions. Uses of Information and Communication Technologies (ICT) are usually actions that belong to a traditional repertoire of human action; with ICT traditional actions can be performed much more efficiently and relatively independently of previous constraints in space and time. At the same time, this is conducive to the individual losing sight of what he/she is actually doing, which is a condition for being a moral agent, charged with ethical responsibility. The IoT may embed the technology in the environment in such a way that in many cases the user may even not know that he/she is interacting with technology.

The comfort may bring along some worries in the form of people's concerns regarding ethical issues such as right or wrong actions by things implicating into their privacy breach, unauthorised tracking, illegal monitoring, trust relationship, safety, and security. Weiser in his seminal paper argued[8]:

> *"The most profound technologies are those that disappear. They weave themselves into the fabric of everyday life until they are indistinguishable from it".*

The IoT envisages a deeply interconnected world beyond our imagination. The technological developments for the IoT are quite visible but ethics seems to be supressed. This is truly reflected in a quote by Ernest Benda[9]:

> *"The problem is the possibility of technology taking on a life of its own, so that the actuality and inevitability of technology creates a dictatorship. Not a dictatorship of people over people with the help of technology, but a dictatorship of technology over people".*

If we look at the technological developments in the recent past, we observe that technology helps us accomplishing complex task in a simpler and efficient manner. In a way, technology has become inevitable for us because people mostly think in terms of involving any available technology to help them doing their tasks. In the IoT, it is expected that billions of devices connected to the Internet will easily out number many times the total human population on earth. In such situation, technology not only becomes inevitable for people but also their daily living may be dictated according to the advancements in technology.

8 Weiser, M.: The Computer for the 21st Century. Scientific American, vol. 265, no. 3, (1991) 66-75.

9 Benda, E.: German Federal Constitutional Court (Chief Justice), on the court's decision to stop the 1983 census and create the novel basic right on 'Informational Self- Determination'. Cited by Rob Van Kranenburg, Ethics Report Venice IoT week, (2012).

Ethical Assessment

Accessing the ethical aspects of the IoT for technologist can be a challenging task. One can use analytic approach of philosophy to understand the moral problems of the technology[10]. While accessing the ethical aspects of the IoT in eHealth, the questions presented by Mason et. al. can give good focus to ethical reasoning[11]:

> *"(a) Who is the agent? (b) What action was taken or is being contemplated? (c) What are the results or consequences of that action? (d) Are those results fair or just?"*

We present the distinguishing characteristics of the IoT that may help us to answer the above questions. The IoT is characterised by some distinguishing features[12], such as heterogeneous, ubiquitous, anonymous, dynamism, intelligence, communication, distributed environment, uncertainty, autonomous, miniaturisation, and virtual identities, etc. The fundamental characteristics of the IoT are interconnectivity between things, things-related services within the constraints of things, dynamic changes in the environment and in the state of devices, and heterogeneity. The high level requirements for the IoT are identification-based connectivity, autonomic networking, autonomic service provisioning, location based capabilities, privacy protection, and security[13]. In the rest of this section, we put forward and analyse the ethical implications of specific features and characteristics of the IoT in the eHealth domain.

Heterogeneous

The IoT in eHealth can establish a heterogeneous network environment connecting things (sensors, smartphones, tablets, computers, etc.) using various operating systems, hardware, software, and protocols across multiple networks. In such a heterogeneous environment, sometimes network boundaries may become unknown making linkability a major ethical concern. Linkability here means to associate information with specific thing in the IoT. For instance, difficulties in terms of knowing about data linkability may result in deniability or non-repudiation by things. In order to strengthen the accountability mechanisms in the IoT, a comprehensive identity management system may counter the problem.

Ubiquitous

The IoT in eHealth envisions a ubiquitous environment providing anytime and everywhere connectivity concept for things. Due to ubiquity, things can be vulnerable against misuse cases of monitoring, tracking, and marketing technologies. Imagine a scenario where our personal belongings (things) equipped with electronic tags and sensors communicating with other things. For instance, medical sensors attached to a patient's body transmitting health parameters, communicating with our personal belongings in handbag. Although electronic tags and sensors may bring comfort in our lives but it may reveal our personal information and thus affecting privacy.

Anonymous

Anonymity refers to namelessness. Although anonymity can be quite useful to address privacy and confidentiality issues for the IoT in eHealth, but at the same time it may create accountability issues. Anonymity may allow bad people to hide themselves by masking their identities. Cyber bullying is an important ethical aspect related to anonymity. Although face-to-face interactions has been an accepted practice in societies to establish trust among people, but at the same time anonymity can be used as a tool in undemocratic societies to express views anonymously that may save lives. However, people with bad intentions may exploit anonymity feature

10 Helping ICT professionals to assess ethical issues in new and emerging technologies, http://www.bcs.org/upload/pdf/assessing-ethical-issues.pdf.

11 Mason, R., Mason, F., Culnan, M.: Ethics of Information Management, SAGE series on business ethics, vol.2 (1995).

12 Hoven, J. V. D.: Fact sheet- Ethics Subgroup Internet of Things - Version 4.01, Delft University of Technology, European commission (2012) 1-21.

13 Recommendation ITU-T, Y.2060, Overview of Internet of Things, 06/2012.

to hide themselves while trying to harm patients in an eHealth system. Hence, anonymity is a challenge and a trade-off for the standard making organisations.

Dynamism

The IoT in eHealth can be considered dynamic not only in terms of its underlying technologies but also in terms of data sources, patient's behaviour, environment, and applications. The dynamic features of the IoT creates dynamic environment that demands the ethical considerations to be dynamic as well. In our opinion, context awareness becomes a key factor in such dynamic environment to understand the ethical implication of a particular action. For instance, if we treat some action ethically correct in a particular context, but due to dynamic network environment and changed context that same action can turn into an unethical action. To further illustrate the case, we consider remote patient monitoring scenario in the IoT, where sensors are attached to a patient's body monitoring health parameters. Suppose two patients 1 and 2 are in close vicinity to each other at some place. In a general context, the communication between the sensors of these patients may be treated ethically wrong due to the privacy concerns of patients. However, if the sensors of patient 1 are unable to transmit data due to low battery power or transmission may lead to further drain in battery. In such context, the sensors of patient 1 may send data through the sensors of patient 2. Due to the changed context, this action may now be treated ethically correct provided the sensitivity of not transmitting the data at all. The situation can become more complex if sensors of patient 1 cause battery drain of patient 2 sensors, resulting in no transmission of own data.

Intelligence

Embedding intelligence into things enables the IoT to turn an ordinary object into a smart thing. The smart things in the IoT may create a smart eHealth system. Due to the inflow of smart technologies, patients may find themselves restrain by the technology confining their freedom. Although smart things may help patients to overcome the barriers of time and place in accomplishing a task, but the smart things also have monitoring and recording capabilities. The actions of patients including their movements, purchases, browsing habits, and work habits may be somehow recorded. This implies that actions may become traceable leading into privacy issues or invading patient's freedom.

Communication

Anytime and anywhere connectivity concept in the IoT demands successful transfer of patient's information. The smart things may generate huge amount of patient's data. The usual way to protect confidentiality of the sensitive information is to use suitable security mechanisms. However, things in the IoT have resource constraints and implementing complex security mechanisms can be cumbersome. Thus, communication requirements sometimes may force to compromise on security requirements. Such cases can be disastrous for privacy and confidentiality concerns of a patient. For instance, to address confidentiality, encryption is a popular technique for which there are number of good cryptographic algorithms already available. Mostly the strength of such algorithms relies upon the complexity, and size of cryptographic keys. However, things in the IoT have constraints in terms of energy, processing power, and storage capacity. Thus, sometimes it may be difficult to use these algorithms that may result in a compromise of privacy or confidentiality of a patient.

Distributed Environment

The huge amount of patients' data, large number of things, and mobility features envisage a distributed environment in the IoT. The governance and management of distributed environment can be a challenging task to hold someone responsible for a particular action. The distributed environment in the IoT may pose several challenges while holding someone responsible for several actions such as, modification of software or firmware

causing harm to a patient's data and system, illegal retrieval of patient's data, and unauthorised access to remote medical system. Hence, the accountability mechanism is a key to tackle non-repudiation related issues[14].

Uncertainty

The complex environment of the IoT can raise many uncertainties in the mind of patients. Patients may not be certain about the flow and handling of their information. When a remote medical centre receives patient's data, uncertainty about data origin, and uncertainty regarding data correctness. Patients may be uncertain regarding with whom and what information is shared. The uncertainty about unknown surveillance may cause discomfort and uneasiness to patients in their freedom of movement.

Autonomous

The smart things in the IoT may not only interact with patients but also autonomously exchange information among them. Things may also react autonomously to the events with or without direct involvement of patients. The autonomous act of smart things may affect the moral rights and obligations of patients. For instance, when things do the shopping by themselves such as, photocopying machine orders the papers itself or a doll orders its new cloths autonomously[15]. Similarly, smart things may order unnecessary stuff that can have monetary damage for patients. To fix the responsibility of business transaction in such cases can be a challenging problem.

Miniaturisation

The miniaturisation of computer technology in the IoT will possibly integrate the smart objects much more into our daily living. The traditional computer technology may vanish due to miniaturisation in technology. Somehow we will be in a scenario where patients communicate with smart objects and smart objects communicating with each other. This kind of environment may have social implications on society such as transparency, dependability, acceptability, accountability, and reliability. For instance, consider a surveillance case in the IoT. The miniaturisation in technology has already produced nearly invisible cameras that bring forward an interesting question: "How much 'life logging' could you tolerate[16]?"

Virtual identities

In the IoT, unique identification number of things embedded in invisible tags would allow consumers to access the virtual representation of things in information world. This information world could provide information to the user about thing such as product review, ingredients, and links to the shop selling the item. Things will be identified by virtual identities, whether such things are people, device, software, or a service. The digital representation of things will be in the form of virtual identity where things may have many virtual identities representing various personas and aspects of their services. According to Roman[17] et. al.:

> *"In the IoT vision, every physical object has a virtual component that can produce and consume services. Such extreme interconnection will bring unprecedented convenience and economy, but it will also require novel approaches to ensure its safe and ethical use".*

In our opinion, it is very important to consider that, what implications it may have when patients interact with machines instead of with people even without knowing it.

14 Xiao, Z., Kathiresshan, N., Xiao, Y.: A survey of accountability in computer networks and distributed systems Security and Communication Networks, John Wiley & Sons, Ltd, (2012) 1-26.

15 Bohn, J., CoroamÄƒ, V., Langheinrich, M., Mattern, F., Rohs, M., Weber, W., Rabaey, J., Aarts, E. (Eds.) Social, Economic, and Ethical Implications of Ambient Intelligence and Ubiquitous Computing Ambient Intelligence, Springer Berlin Heidelberg, (2005) 5-29.

16 Hudson, A.: How much 'life logging' could you tolerate? BBC click, (2013), http://www.bbc.co.uk/news/technology-22193299.

17 Roman, R., Najera, P., Lopez, J.: Securing the Internet of Things. Computer, vol. 44, no. 9, (2011) 51-58.

Ethical Discussion

The IoT presents the concept of smart world through the integration of smart objects into our daily living, such as smart cities, smart environment, smart logistics, smart industrial control, smart agriculture, smart animal farming, and smart e-Health. Here, the term smart refers to an environment where things have certain capabilities such as sensing, monitoring, computing, intelligence, and decision making. These applications can help us in effective energy management, enhanced healthcare, and more independent living. On the other hand, if we look closely at these environments, we see sensors monitoring and collecting bundles of data that have many identity and privacy based implications. Gérald Santucci in his speech on the governance of the IoT said[18]:

> *"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".*

Rafael Capurro and Michael Nagenborg performed ethical evaluation of European institutes to estimate the likelihood of ethical issues due to emerging information and communication technologies[19]. Amongst their findings they indicated the potential conflict with the values and principles of EU charter, the opinion of European group on ethics in science and new technologies, other national bio-ethics committees, and other official EU documents. They included human dignity, freedom of research, privacy, and justice for their analysis. They concluded that emerging technologies have high likelihood of becoming an ethical issue such as ambient intelligence, human machine symbiosis, neuro electronics, robotics, affective computing, artificial intelligence, and bioelectronics. Interestingly all of these technologies are part of the IoT. They also highlighted the lack of ethical research on animals and environment as they think that the recent efforts are mainly human centred.

However, many professional societies, organisations, and technology related standard making organisations consider ethics as an essential element in technology development as it is reflected in their code of ethics. In the IEEE (Institute of Electrical and Electronics Engineers) code of ethics[20], they commit themselves, "to accept responsibility in making decisions consistent with the safety, health, and welfare of the public, and to disclose promptly factors that might endanger the public or the environment; to improve the understanding of technology; it's appropriate application, and potential consequences; or after full disclosure of pertinent limitations; to seek, accept, and offer honest criticism of technical work; to acknowledge and correct errors, and to credit properly the contributions of others; to treat fairly all persons regardless of such factors as race, religion, gender, disability, age, or national origin". Also, according to the ACM (Association for Computing Machinery) code of ethics[21] and professional conduct, "avoid harms to others, be fair and take action not to discriminate, respect the privacy of others, and honour confidentiality".

An important aspect inside the IoT objective is to narrow the rich and poor gap[22]. That implies that the opportunity to access the IoT must not treat rich and poor differently. However, there are countries where families will have difficulties to afford the smart devices. The inability to purchase smart devices may keep them away from the goods of the IoT.

---

18 Kranenburg, R. J., Jaromil D. R., Carrez, F.: The Internet of Things Initiative (2012) 1-66. http://www.iot-i.eu/public/public-deliverables/d2.5-ethicsinside.eu/at_download/file.

19 Carsten, B. S.: Ethical issues of emerging ICT applications, the magazine of the European innovation exchange, issue 6, (2011) 1-36, http://www.ethics.ccsr.cse.dmu.ac.uk/etica/EIEX06ETICA2.pdf.

20 IEEE Code of Ethics. (2006), http://www.ieee.org/about/corporate/governance/p7-8.html.

21 ACM Code of Ethics and Professional Conduct, (2013), http://www.acm.org/about/code-of-ethics/#sect1.

22 The Internet of Things. https://sites.google.com/a/cortland.edu/the-internet-of-things.

Conclusion

The future of the current Internet is the Internet of highly connected digital world where patients will be fenced by tiny smart things. In such an environment the actions taken by things to comfort a patient may have serious ethical implications as well. While people are keen to develop standards and technologies for the IoT, the ethical aspects of these developments must not be ignored for later analysis rather it may be incorporated in the system development life cycle. The claimed benefits of the IoT may not be realised, unless ethical implications of such claims on people, society, and environment are justified. Also, there is a strong need to formulate solutions to potential ethical issues in the IoT before it is irreversibly adopted by society.

References

Evans, D.: Internet of Everything (IoE), CISCO Blogs, (2013), http://blogs.cisco.com/ioe/.

Sundmaeker, H., Guillemin, P., Friess, P., and Woelfflé, S.:Vision and challenges for realising the Internet of Things, Cluster of European Research Projects on the Internet of Things—CERP IoT, (2010) 1-236.

Future Internet Strategic Research Agenda, Version 1.1, European Future Internet X-ETP Group, (2010) 1-73.

Vermesan, O. et al.: Internet of Things Strategic Research Roadmap 2011, European Research Cluster on the Internet of Things, (2011) 1-44.

Atzoria, L., Ierab, A., and Morabito, G.: The Internet of Things, A survey, Computer Networks (54), (2010) 2787-2805.

Habib, K., Torjusen, A., and Leister, W.: A Novel Authentication Framework Based on Biometric and Radio Fingerprinting for the IoT in eHealth, (2014) 32-37.

Leister,W., and Schulz, T.:Ideas for a trust indicator in the Internet of Things, (2012), 31-34.

Weiser, M.: The Computer for the 21st Century. Scientific American, vol. 265, no. 3, (1991) 66-75.

Benda, E.: German Federal Constitutional Court (Chief Justice), on the court's decision to stop the 1983 census and create the novel basic right on 'Informational Self- Determination'. Cited by Rob Van Kranenburg, Ethics Report Venice IoT week, (2012).

Helping ICT professionals to assess ethical issues in new and emerging technologies, http://www.bcs.org/upload/pdf/assessing-ethical-issues.pdf.

Mason, R., Mason, F., Culnan, M.: Ethics of Information Management, SAGE series on business ethics, vol.2 (1995).

Hoven, J. V. D.: Fact sheet- Ethics Subgroup Internet of Things - Version 4.01, Delft University of Technology, European commission (2012) 1-21.

Recommendation ITU-T, Y.2060, Overview of Internet of Things, 06/2012.

Xiao, Z., Kathiresshan, N., and Xiao, Y.: A survey of accountability in computer networks and distributed systems Security and Communication Networks, John Wiley & Sons, Ltd, (2012) 1-26.

Bohn, J., CoroamÄƒ, V., Langheinrich, M., Mattern, F., Rohs, M., Weber, W., Rabaey, J., and Aarts, E. (Eds.) Social, Economic, and Ethical Implications of Ambient Intelligence and Ubiquitous Computing Ambient Intelligence, Springer Berlin Heidelberg, (2005) 5-29.

Hudson, A.: How much 'life logging' could you tolerate? BBC click, (2013), http://www.bbc.co.uk/news/technology-22193299.

Roman, R., Najera, P., and Lopez, J.: Securing the Internet of Things. Computer, vol. 44, no. 9, (2011) 51-58.

Kranenburg, R. J., Jaromil D. R., and Carrez, F.: The Internet of Things Initiative (2012) 1-66. http://www.iot-i.eu/public/public-deliverables/d2.5-ethicsinside.eu/at_download/file.

Carsten, B. S.: Ethical issues of emerging ICT applications, the magazine of the European innovation exchange, issue 6, (2011) 1-36, http://www.ethics.ccsr.cse.dmu.ac.uk/etica/EIEX06ETICA2.pdf.

IEEE Code of Ethics. (2006), http://www.ieee.org/about/corporate/governance/p7-8.html.
ACM Code of Ethics and Professional Conduct, (2013), http://www.acm.org/about/code-of-ethics/#sect1.
The Internet of Things. https://sites.google.com/a/cortland.edu/the-internet-of-things.

Bernhard Stengel:

Ethische Überlegungen zu Smart Home

Abstract:

"Smart Home" is used as a buzzword to term a wide scope of home automation. In this paper the focus is on systems connected to the internet, being primarily operated by mobile ICT devices. When viewing systems already available, those being available in Germany take centre stage. In a general point of view the new human interface to devices is compared to that of old-fashioned devices. Regarding social togetherness, the topics of multi user mode and monitoring of homes are discussed. It is not sure that all persons living in the home get fair access to the new technology. Furthermore, when persons being present at different locations are able to operate the same device, there is the task to synchronize the actions. The main focus of monitoring is on suspect strangers approaching from outside, but it also could be applied inside in a questionable manner. Control of home infrastructure by algorithms raises questions of paternalism.

Agenda:[1]

Author:

Dr. Bernhard Stengel:
- Rahel-Straus-Weg 7, 81673 München, Germany
- ☎ + 49 - 89 – 43 58 85 91 , ✉ bernhard.stengel@plus.cablesurf.de

[1] Updated version as of 01.06.2015

ISSN 1614-1687

Der vorliegende Artikel behandelt ethische Aspekte internetbasierter Wohnungsautomatisierung, welche einen Sonderfall des „Internet der Dinge" (IoT: Internet of Things) darstellt. Als Mark Weiser 1991 eine neue Ära des Ubiquitous Computing (UC) proklamierte, wonach viele Geräte mit höchst unterschiedlicher Funktionalität vernetzt sind,[1] gab es bereits viele automatisierte Dinge, die Embedded Computer enthielten. Er rechnete sie jedoch nicht dem UC zu, sondern sah sie nur als dessen Vorboten (*harbingers*) an, weil sie noch nicht miteinander kommunizierten.[2] Die aktuell verfügbaren Smart Home-Systeme kommen Weisers Vision näher, aber auch sie entsprechen ihr noch nicht wirklich. Während philosophische Untersuchungen zur Vision des UC einen künftigen Stand der Technologie zum Thema haben, bei der die Wahrung der Autonomie des Menschen eines der Grundprobleme ist,[3] interessiert sich der vorliegende Artikel für konkrete, bereits existierende Systeme, insbesondere für in Deutschland verfügbare. Angesichts der Unübersichtlichkeit und hohen Dynamik der erst am Anfang stehenden internetbasierten Technologie wird keine Normbegründung im strengen Sinne vorgelegt; teilweise entspricht der Ansatz einer Klugheitsethik. Der Artikel nimmt keine endgültigen Abwägungen vor, sondern beschränkt sich auf die Vorstellung möglicher Problempunkte sowie einige Überlegungen zur Mensch-Maschine-Schnittstelle. Er nimmt auch solche Aspekte in den Blick, die bei einem auf Grundlagenprobleme fokussierten Diskurs unberücksichtigt bleiben. Der Abschnitt über Obsoleszenz ist ein Beispiel dafür, dass manche Themen nicht einer bestimmten Bereichsethik zuzuordnen sind, sondern dass eine Perspektive sinnvoll ist, die über der gängigen Einteilung der Bereichsethiken steht.

Gebäudeautomatisierung ist bei manchen großen Gebäuden, z.B. Bürogebäuden, bereits seit vielen Jahren im Einsatz, wobei die Datenkommunikation über verdrahtete Datenbusse erfolgt. Solche autarken Automatisierungslösungen, die auch für Wohnhäuser erhältlich sind, können ergänzend einen Internetanschluss haben, er wird jedoch nicht für die eigentlichen Funktionen benötigt. Im Unterschied dazu gibt es neuerdings Systeme, die permanent mit dem Internet verbunden sein müssen. Für datenbus-basierte Automatisierung existieren etablierte Standards (z.B. KNX). Dagegen sind für internetbasiertes Smart Home, wie im Bereich IoT insgesamt, die technischen Schnittstellen nicht vereinheitlicht, was die Vielfalt der miteinander vernetzbaren Geräte deutlich einschränkt. In beiden Varianten der Wohnungsautomatisierung werden manche Funktionen regelbasiert ohne unmittelbares menschliches Eingreifen ausgeführt, und außerdem stehen dem Menschen Möglichkeiten der Fernbedienung zur Verfügung.

Für den Ausdruck Smart Home existiert bisher keine allgemeingültige Definition;[4] er meint eine Technologie für private Wohnungen (Eigenheime, Mietwohnungen etc.), wodurch u.a. Heizung, Beleuchtung und Haushaltsgeräte wie Waschmaschinen mittels Vernetzung zu „intelligenten" Gegenständen werden.[5] Smart Home ist ein Modewort, das teils unspezifisch, teils mit Fokus auf die etablierte datenbus-basierte, teils mit Fokus auf die neue internetbasierte Technologie verwendet wird. Das folgende Kapitel behandelt speziell internetbasiertes Smart Home; die Angaben in den weiteren Kapiteln gelten teilweise auch darüber hinaus.

Internetbasiertes Smart Home

Überblick

In diesem Kapitel geht es um internetbasierte Produkte wie QIVICON oder RWE SmartHome, die preiswerter sind als datenbus-basierte Heimvernetzung. Dabei befindet sich in der Wohnung eine Steuereinheit,[6] die mit

[1] Weiser, Mark: The Computer for the 21st Century

[2] Weiser, Mark / Brown, John Seely: The coming age of calm technology

[3] Zum Beispiel Wiegerling, Klaus: Philosophie intelligenter Welten: vgl. insbesondere 13 und 24

[4] BITKOM: Heimvernetzung. 22

[5] Der Ausdruck wird nicht nur für die Technologie, sondern auch für eine entsprechend ausgestattete Wohnung verwendet.

[6] Es gibt auch Systeme wie z.B. Home Connect aus dem Hause Bosch, die keine solche Steuereinheit benötigen.

ISSN 1614-1687

mehreren „smarten" Geräten (Sensoren und Aktoren) drahtlos kommuniziert. Sie ist permanent über Internet mit einem Computer des Diensteanbieters des Smart Home-Systems verbunden, wo Anwenderprogramme laufen und die Daten mit Hilfe der Cloud-Technologie verwaltet werden. Die Inbetriebnahme erfolgt oftmals durch den Anwender selbst, ohne dass professionelle Unterstützung vor Ort erfolgt. Die Benutzer kommunizieren mit dem System hauptsächlich über mobile Kommunikationsgeräte wie Smartphones oder Tablet-Computer. Abgesehen von diesen können meist nur solche Geräte eingebunden werden, die dasselbe Firmenlabel tragen bzw. zur selben Firmenallianz gehören, wodurch sich ein geschlossener Charakter ergibt. Außerdem besteht keine freie Wahl eines Diensteanbieters, sondern der Verkauf der Hardware und der anschließende Betrieb sind miteinander gekoppelt. Hinsichtlich der technischen Konfiguration ist Weisers Vision von UC noch nicht erreicht, weil in einer hierarchischen Struktur viele Entscheidungen auf dem zentralen Computer des Systemanbieters getroffen werden, während die „Dinge" nur in eingeschränktem Maße „intelligent" sind. Darüber hinaus besteht ein wichtiger Unterschied darin, in welchem Umfang der Mensch heute noch autonom über ICT-Geräte eingreifen kann bzw. als Benutzer darüber Kontrolle hat, was per Algorithmus im Hintergrund ausgeführt wird.

Smart Home überschneidet sich mit weiteren IoT-Anwendungsgebieten. So hat Smart Meter die Etablierung „intelligenter" Stromzähler in Kombination mit flexiblen Stromtarifen zum Ziel. In Zukunft könnten vernetzte Waschmaschinen einerseits durch den Benutzer von überall aus gestartet werden, wenn es ihm zeitlich am günstigsten passt; andererseits könnten sie durch Algorithmen gestartet werden, wenn der Stromtarif am günstigsten ist. Dem Benutzer wird ein Bündel künftiger Vorteile angepriesen, von denen manche vom Konzept her nicht ideal zusammenpassen.

Funktionelle Zuverlässigkeit

Weisers Vision, Computer würden derart „verschwinden", dass wir die Dinge unbeschwert ohne Nachdenken benützen können, setzt ihr fehlerfreies Funktionieren voraus. Wenn Fehlfunktionen zu Schäden führen, stellt sich die Frage nach Verantwortung und Schadenersatz. Bei Produkthaftung und Verbraucherschutz handelt es sich hauptsächlich um rechtliche Themen, aber die Frage nach einem fairen Gleichgewicht bei der Zuweisung von Verantwortlichkeit betriff auch die Ethik. Bei internetbasierten Systemen ist die Situation sowohl in technischer als auch in rechtlicher Hinsicht komplexer als bei Einzelgeräten; z.B. wird ggf. der Kauf und die anschließende Nutzung der Dienste durch unterschiedliche Verträge geregelt. Darum ist der Kunde im Schadensfall eventuell in einer schwächeren Position im Vergleich zu unvernetzten Einzelgeräten.

Seit den 1990er Jahren hat die Anzahl von Hackerangriffen deutlich zugenommen. Im Fall von Smart Home besteht die Gefahr der Manipulation der Hausinfrastruktur sowie des Diebstahls sensibler Daten (z.B. Abwesenheitszeiten von der Wohnung) aus dem Cloud-Datenzentrum des Diensteanbieters. Ein Anbieter fordert vom Kunden Schutzmaßnahmen gegen Viren ein, schließt andererseits aber eigene Haftung im Fall von „Virenbefall" ähnlich wie Naturkatastrophen als Höhere Gewalt aus.[7] Eine Sicherheitsempfehlung des Landeskriminalamts (LKA) Nordrhein-Westfalen lautet: „Verbinden Sie Ihre Geräte nur dann mit dem Internet, wenn dies wirklich nötig ist, z.B. für Updates oder wenn Sie entsprechende Funktionen nutzen wollen."[8] Andererseits sieht das LKA Stand 2014 keinen Anlass, vor bestimmten Systemen zu warnen.[9] Angesichts unübersichtlicher Einschätzungen hinsichtlich permanenter Anbindung von Haustechnik an das Internet dürfte es für den künftigen Anwender hilfreich sein, sich vor dem Kauf mit klärenden Anfragen u.a. an seine Versicherung zu wenden.

[7] Swisscom: Allgemeine Geschäftsbedingungen Interactive Home Services von Swisscom

[8] Landeskriminalamt Nordrhein-Westfalen: Smart Home und Connected Home. 3

[9] Mail des LKA NRW vom 24.11.2014 an den Autor des Artikels

Obsoleszenz

Obsoleszenz bedeutet, dass ein Produkt vor Ablauf der üblichen Lebensdauer veraltet oder funktionsunfähig und somit zu Abfall wird.[10] Bei Smart Home werden langlebige Haushaltsgeräte wie Waschmaschinen[11] und Kommunikationsgeräte von deutlich kürzerer Lebensdauer und mit kürzeren Innovationszyklen funktionell miteinander verbunden. Es ist unsicher, wie lange die App zum Betrieb des Haushaltsgeräts für neue Smartphones verfügbar sein wird. Ebenso ist unsicher, ob nach etlichen Jahren die passende Haushaltsgeräte-App auch für dasjenige Smartphone erhältlich sein wird, das dem dann aktuellen Kommunikationsverhalten des Benutzers optimal entspricht. Letzteres ist medienethisch insofern relevant, weil ggf. langlebige „smarte" Haushaltsgeräte den Benutzer bei der künftigen Wahl seines Kommunikationsgerätes einschränken und zu Kompromissen veranlassen. Bedeutsamer dürfte aber das umweltethische Problem zusätzlichen Mülls sein, welcher durch eine neue Variante funktionaler Obsoleszenz entsteht. Ein Unsicherheitsfaktor dabei ist auch die Verfügbarkeit des zugehörigen Programms auf dem Rechner des Diensteanbieters, denn manche Nutzungsbedingungen enthalten das Recht auf entschädigungslosen Wegfall von nicht mehr zeitgemäßen Leistungsmerkmalen. Es könnte den Nutzern mehr Unabhängigkeit und Planungssicherheit bringen, wenn auch vom Hersteller unabhängige Diensteanbieter tätig werden könnten; eine solche Entwicklung ist jedoch nicht absehbar.

Big Data

Durch die Systemarchitektur, wonach wichtige Anwendungsprogramme nicht lokal, sondern unter der Regie des Diensteanbieters laufen, werden viele private Daten in dessen Cloud-Datenhaltung gespeichert. Manche Anbieter sehen in ihren datenschutzrechtlichen Einwilligungen vor, dass die „personenbezogenen Daten" zu Werbezwecken ausgewertet werden dürfen, zu denen neben den Registrierungsdaten auch die erteilten Befehle zur Steuerung der Hausgeräte gehören können.[12] Falls der Benutzer entscheiden kann, ob die Geräte Daten senden oder nicht, ist die Ablehnung mit dem Verzicht auf gewisse Funktionen verbunden;[13] allerdings ist diese Entscheidungsmöglichkeit nicht selbstverständlich. Es stellt sich die Frage, für welche Funktionen die Preisgabe von Daten angemessen erscheint; aus der Protokollierung der Gerätebedienung lassen sich u.a. Angaben über den Tages- und Wochenrhythmus des Benutzers ableiten.

Ein neues digitales Weltverhältnis

„Entörtlichte" Bedienung

Wenn „smarte" Geräten automatisch miteinander kommunizieren, entfällt (abgesehen von der Änderung einiger Parameter) die Bedienung durch den Menschen. Nachfolgend wird die menschliche Bedienung durch virtuelle Tasten auf einem Smartphone-Menü betrachtet, wodurch es möglich ist, von überall aus Geräte zu Hause anzusprechen. Der physische Schalter eines altbekannten Gerätes wie z.B. einer Kaffeemaschine ist ein Teil des Gerätes selbst, wobei der Sachverhalt des Zusammengehörens intrinsisch eine kontextuelle Information enthält. Bei der Bedienung per Smartphone verschwinden gewissermaßen die physischen Schalter auf dem „Ding" und werden durch virtuelle auf dem Kommunikationsgerät ersetzt.[14] Dabei kommt es zu einem Verlust der ursprünglichen kontextuellen Information, der dadurch kompensiert wird, dass das Gerät benannt und über seinen Namen angesprochen wird. Auf einer für den Benutzer verborgenen Ebene geschieht dies über seine technische Geräteadresse, auf der Benutzerebene durch den vom Benutzer gewählten Gerätenamen. In der Telekommunikation ist es selbstverständlich, dass entfernte Partner durch Adressen (Telefonnummern, Email-Adressen

[10] Sperlich, Kristine / Oehme, Ines: Fachgespräch "geplante Obsoleszenz". 2

[11] Lebensdauer von Waschmaschinen mit Umweltzeichen mindestens 10 Jahre, vgl. Sperlich, Kristine / Oehme, Ines: Fachgespräch. 9

[12] Vgl. z.B. Home Connect: Nutzungsbedingungen für das Home Connect System

[13] Vgl. Home Connect: FAQs zu Home Connect

[14] Manche internetbasierten Geräte können sowohl offline per Geräteschalter als auch online betrieben werden, andere nur online.

etc.) ausgewählt werden, aber die betreffende Technik hat die Überwindung großer Distanzen als ihren eigentlichen Zweck. Nun werden Geräte unserer unmittelbaren Wohnumgebung in die „Entörtlichung" einbezogen, und so stellt die Ersetzung physischer Geräte-Schalter durch virtuelle Menü-Tasten eine neue Stufe eines digitalen Weltentwurfs durch den Menschen dar.[15]

Die weltweite Erreichbarkeit geht einher mit einer grundsätzlich geänderten Bedienweise. Eine praktische Konsequenz davon lässt sich durch das Beispiel einer großen Wohnung verdeutlichen, in der sich im Erdgeschoss und im ersten Stock jeweils eine Kaffeemaschine (K_EG bzw. K_1) befindet. Wer vor K_EG steht, wird bei manueller Bedienung definitiv dieses Gerät einschalten, nicht K_1 im Stockwerk darüber. Bei Bedienung per Smartphone ist es möglich, K_1 von überall aus einzuschalten, auch dann, wenn man unmittelbar vor K_EG steht. In einigen Fällen ist es tatsächlich gewollt, in anderen handelt es sich um eine Fehlbedienung als Folge der erweiterten Möglichkeit. – Die neue Technologie erlaubt, Geräte auf unterschiedliche Weise auf Menüs „abzubilden"; ein Menü könnte alle Geräte eines Zimmers oder alle Kaffeemaschinen zusammenfassen. (Allerdings müssen nicht alle Möglichkeiten in einem käuflichen System zur Verfügung stehen.) Darüber hinaus könnte es sein, dass nicht jeder Bewohner einer Wohnung Zugriff auf alle physisch vorhandenen Geräte hat, sondern dass ggf. unterschiedliche Benutzergruppen spezielle an sie angepasste Menüs verwenden. Die neue Mensch-Maschine-Schnittstelle kann also deutlich mehr, als die Geräte aus der Ferne anzusprechen. Ihre künftige Weiterentwicklung sollte auf verantwortungsvolle Weise erfolgen.

Zur Fernbedienung sollte die Frage erlaubt sein, ob ihr konsequenter Einsatz sinnvoll ist. Christopher Mims weist darauf hin, dass die bisherige „Nutzeroberfläche" eines Hauses bereits ziemlich gut funktioniert, und fragt: „Wie revolutionär wäre zum Beispiel ein Lichtschalter, wenn man die Lampen vorher nur über ein Smartphone hätte anschalten können?"[16] Es mag nützlich sein, während einer Abwesenheit Statusmeldungen von zu Hause abzurufen. Andererseits steht das Szenario, morgens nach dem Wecker-Läuten vom Schlafzimmer aus per Smartphone die Kaffeemaschine in der Küche einzuschalten, dem Szenario gegenüber, sie durch programmierte Zeitvorwahl zu starten. Neuere Einzelgeräte ohne Internetanschluss haben diese Möglichkeit; sie vermeiden die typischen IoT-Probleme wie z.B. Big Data.

Der ständige Zugriff von überall auf das Haus ist auch unter dem Aspekt des Überangebots an Möglichkeiten zu sehen, wobei dasjenige Überangebot um eine zusätzliche Dimension erweitert wird, welches bisherige Medien bereits bereithalten. So gilt nun erst recht der Hinweis von Rafael Capurro auf eine neue Form der Lebenskunst und das Lernen von Genügsamkeit (*Askese*).[17]

Weiser sprach in seinem eingangs erwähnten Artikel davon, dass UC zu einem „Verschwinden der Computer" führen werde. Da das Smartphone als Kommunikationsgerät mit seinem Computerchip eine neue Bedeutung als menschliche Schnittstelle zu den Dingen erhält, könnte dieser Ausdruck ohne eine nähere Erläuterung missverstanden werden. Weiser bezieht ihn auf die menschliche Psychologie, nicht auf Technologie.[18] In seiner Vision kommen einerseits ICT-Geräte vor, deren Bedienung für den Menschen selbstverständlich ist; andererseits gibt es weniger zu bedienen, weil die Computer viele Aufgaben „unsichtbar" erledigen. In unserem Kontext trifft der Ausdruck „Verschwinden der Computer" unter der Prämisse zu, dass der Mensch die neue Semantik virtueller Schaltflächen oder andere neue Bedienweisen ausreichend gut gelernt hat, so dass sie für ihn selbstverständlich geworden sind.

Bezugnahme durch Hinzeigen

Die Linguistik und die Sprachphilosophie unterscheiden eine Bezugnahme mit Hilfe von Eigennamen von derjenigen auf deiktische bzw. indexikalische Weise mittels Worten wie „dieses" oder „hier". Zum Beispiel kann

[15] Zum Zusammenhang zwischen Weltentwurf und Internetethik vgl. Capurro, Rafael: Existenzontologie: Operari sequitur esse

[16] Mims, Christopher: Das vernetzte Haus verkompliziert nur das Leben

[17] Capurro, Rafael: Leben im Informationszeitalter. 44

[18] Weiser, Mark: The Computer for the 21st Century. 66

man eine Person, die sich im selben Zimmer aufhält, bitten, das Gerät mit dem Namen „XY" oder „dieses" Gerät einzuschalten. – Zusätzlich zur Menü-Bedienung wäre folgende Bedienweise möglich, die derzeit bei Smart Home nicht üblich ist, aber abgewandelt bei anderen internetbasierten Anwendungen wie Augmented Reality vorkommt: Jedes automatisierte Gerät erhält einen individuellen Code-Aufkleber; der Benutzer wählt das betreffende Gerät aus, indem er mit seinem Smartphone in Richtung der Geräte-Codierung zeigt, wobei ein Sensor den Code erfasst. Aus Perspektive des Benutzers handelt es sich um eine deiktische Bezugnahme auf ein Gerät als „dieses Gerät". Auf der Ebene der technischen Realisierung ist es aber ein Ansprechen über einen Geräte-Code, d.h. einen Eigennamen. Während wir bei menschlicher Kommunikation auf jedes Ding unserer Umwelt zeigen und sprachlich als „dieses Ding" darauf Bezug nehmen können, funktioniert die neue technische Analogie nur mit denen, die per Code eine Adresse erhalten haben. – Es ist zu erwarten, dass es künftig zu einem Nebeneinander neuer Bedienweisen kommen wird (Menü-Tasten für den Fernbereich, Hindeuten im Nahbereich etc.), wobei die Aufgabe entsteht, diese widerspruchsfrei aufeinander abzustimmen, sowohl auf technischer Ebene als auch hinsichtlich der Benutzer-Psychologie.

Wenn IoT und die Ausstattung von Dingen mit Codes voranschreitet, wird dies Auswirkungen auf unser künftiges Weltverhältnis haben. Dann werden wir mittelfristig die Dinge unserer Umwelt wohl in zwei große Gruppen einteilen, nämlich ob wir sie technisch ansprechen können oder nicht. (Nicht jedes Ding mit einer Adresse ist auch für *uns* erreichbar.)

Aspekte sozialen Zusammenlebens

Mehrpersonenbetrieb

Die Smart Home-Technologie führt aus Sicht ihrer Befürworter zu einer Zunahme an Freiheit und Unabhängigkeit. Aber lediglich in Einpersonenhaushalten (ohne Besucher) steht fest, dass alle daran Anteil haben. Bei der Produktwerbung wird Mehrbenutzerbetrieb oft nur in geringem Umfang thematisiert; ein künftiger Anwender sollte darum vor Kauf abklären, ob das Produkt seinen Anforderungen genügt. Dazu gehört, dass der Anbieter das Laden seiner App auf mehrere Smartphones juristisch zulässt und dass er den Begriff des „Dritten", der per Vertrag ausgeschlossen ist, nicht zu strikt auffasst. Andererseits stellt sich auf Benutzerseite die Frage, welche Zugriffsrechte der Hauptbenutzer, der den Vertrag unterzeichnet hat, anderen Personen zugesteht. Die Vergabe abgestufter Zugriffsrechte an unterschiedliche Benutzergruppen ist bei manchen Systemen möglich, aber nicht selbstverständlich. Sie könnte z.B. sicherstellen, dass Kinder ausgewählte, aber nicht alle Geräte einschalten können. Ein Bedarf dazu besteht wohl, weil man einem Kind die Benutzung eines Gerätes nicht so anschaulich verbieten kann, wenn es sich um virtuelle Menü-Tasten anstatt physische Bedienung handelt. Hinsichtlich der Einbeziehung von Besuchern können abgestufte Zugriffsrechte ebenfalls sinnvoll sein. Falls das System zu unflexibel ist, kann es ggf. Gastfreundschaft erschweren.

Von solchen Fragen des grundsätzlichen Zugangs sind die der Koordination beim Ansprechen desselben Geräts durch mehrere Personen zu unterscheiden. Z.B. kann ein Ehepaar für eine konventionelle Waschmaschine die Absprache treffen: Wer zuerst nach Hause kommt, schaltet sie ein. Die neue Fernbedienung ermöglicht einerseits das Einschalten bereits auf dem (meist getrennten) Nachhauseweg, erfordert andererseits aber zusätzliche Koordination. Sollte diese nicht erfolgreich sein, wird ggf. die Hausarbeit noch stärker als bisher einer bestimmten Person zugeordnet.[19] Insbesondere die Funktion, mit einem Knopfdruck alle elektrischen Geräte auszuschalten, kann in Mehrpersonenhaushalten problematisch sein. Wenn z.B. PersonA als letzte das Haus verlassen hat und aus der Ferne diesen Knopf drückt, weil sie unsicher ist ob, sie zuvor alle Geräte ausgeschaltet hat, kann dennoch in der Zwischenzeit ungeplant PersonB nach Hause zurückgekehrt sein und dann ins Dunkle gesetzt werden. Falls Produktwerbung ohne Nennung weiterer Details solche Funktionen anpreist, ist eine Rückfrage nach deren Leistungsfähigkeit angebracht.

[19] Das Problembeispiel mag gekünstelt erscheinen, aber dasselbe gilt auch für viele gängige Beispiele zu den Vorteilen von Smart Home.

Überwachung von Personen

Sicherheit und Überwachung werden nach Ansicht eines Experten in den USA die Hauptanwendungsgebiete von Hausautomatisierung sein.[20] In der Öffentlichkeit fand die Übernahme des Thermostat-Herstellers Nest durch Google große Beachtung; weniger beachtet wurde jedoch das Interesse von Nest am Start-up-Unternehmen Dropcom, einem Hersteller von Überwachungskameras. – Überwachung richtet sich hauptsächlich gegen verdächtige Fremde, sie könnte aber auch innerhalb des Haushalts eingesetzt werden. Ein indisches Automatisierungsunternehmen wirbt mit dem Satz: „Be the commandant of your home even if you are miles away."[21] Da in Indien Einpersonenhaushalte selten sind, geht es wohl nicht um die Kontrolle über eine menschenleere Wohnung, sondern um eine, in der sich Familienmitglieder und ggf. Hausangestellte aufhalten. Bereits existierende patriarchale Familienstrukturen können dadurch verstärkt werden, dass nur das Familienoberhaupt Zugang zu zentralen Funktionen hat und sein Haus jederzeit von überall auf der Welt im Auge behalten kann. Dies könnte auch für konservative Familien in anderen Ländern zutreffen. Deutschland ist einerseits hinsichtlich seiner Rolle als Exportland involviert; andererseits wirbt ein deutscher Hersteller mit der Möglichkeit, die Arbeitszeit einer Putzhilfe zu kontrollieren.[22]

Technische Kommunikation durch Abfrage von Bewegungsmeldern oder das Beobachten über Kameras kann die menschliche Kommunikation auch in solchen Situationen verdrängen, wo letztere angemessener wäre. Wenn z.B. eine Mutter aus der Ferne herausfinden will, ob ihr Kind bereits zu Hause eingetroffen ist, könnte sie entweder telefonisch nachfragen oder per Smart Home die Statusmeldungen des Hauses abrufen. Eine Produktwerbung empfiehlt letzteres, weil sich anderenfalls das Kind beklagen könnte, die Mutter würde ihm nicht vertrauen.[23] Dabei handelt es sich um eine fragwürdige Methode, das Vertrauen nicht zu verlieren, indem man heimlich nicht vertrauensvoll handelt.

Das Verhältnis zwischen Mensch und Computer

Wenn sich die Automatisierungstechnologie an Weisers Vision des UC annähert, wird es mittel- bis langfristig zu einer Vielzahl im Hintergrund ablaufender Algorithmen kommen, die für den Menschen „unsichtbar" sind. Welche Auswirkungen dies auf das Verhältnis zwischen Mensch und Computer haben könnte, kann hier nicht ausführlich dargestellt werden und sei lediglich für den Bereich Energie auf Basis einer vorläufigen Beobachtung diskutiert. Obwohl Smart Home Energieeinsparungen ermöglicht, kann es vorkommen, dass ein hocheffizientes automatisiertes Haus mehr Energie verbraucht. Manche Bewohner gehen nämlich sorglos mit ihr um, in der Annahme, dass die maschinelle Intelligenz alles regelt. Im betreffenden Musterhaus mussten ihnen darum fortlaufend Energiespartipps über IT-Systeme eingespeist werden.[24] Diese Beobachtung ist ein erster Hinweis auf ein komplexes Problem: Weisers Erwartung, die Computer würden in psychologischer Hinsicht für den Menschen „verschwinden", traf in diesem Fall nicht ein. Indem die betreffenden Bewohner die Leistung der Computer überschätzten, wiesen sie ihnen per Zuschreibung eine neue Rolle im Miteinander der Akteure zu; zweitens wiesen ihnen die Systembetreiber die Aufgabe zu, Verhaltenstipps zu geben. Nachdem die Computer über die Wohnung „herrschten", mussten sie anschließend auch die Bewohner beeinflussen. Falls die Computer zusätzlich die Einhaltung der Tipps überprüfen sollten, würde aus Perspektive der Bewohner eine mehrstufige Bevormundung ablaufen. Hinzu kommt: Während die Bewohner des Musterhauses von neutraler Seite mit Tipps versorgt werden, wird wohl künftig bei kommerziellem Betrieb außer rationalen Tipps auch Werbung verschickt. Es wäre ein fragwürdiges Geschäftsmodell, Menschen, die Tipps benötigen, auf diesem Weg empfänglich für Werbung zu machen.

[20] Mims, Christopher: Das vernetzte Haus verkompliziert nur das Leben

[21] Smart Automation: Home Automation

[22] Gigaset elements: Alles Gute zum Weltfrauentag!

[23] Gigaset elements: Alles Gute zum Weltfrauentag!

[24] Borchers, Detlev: Home, sweet smart Home

Für Menschen, die als an Technik Interessierte aktiv die Automatisierung ihrer Wohnung planen und die Leistung der Computer nüchtern einschätzen, trifft das genannte Verhältnis Mensch – Computer nicht zu. Von diesen „Pionieren" lässt sich nicht auf die künftige breite Anwendung extrapolieren, sondern Ausgangspunkt sind jene Musterhaus-Bewohner, die nicht über dessen technische Details nachdenken. Es besteht ein Bedarf, die Auswirkungen der Hausautomatisierung auf das Verhalten und die Einstellungen der Bewohner weiter zu untersuchen, und zwar frei von kommerziellen Interessenkonflikten. Falls sich bestätigen sollte, dass Energieeinsparung in manchen Fällen nur dann effizient funktioniert, wenn Computer neben der Optimierung der „Dinge" auch Einfluss auf die Einstellungen der Bewohner nehmen, wäre dies von ethischer Relevanz. Es könnte nämlich mittelfristig ein fragwürdiger Prozess in Gang kommen, dass Computer das individuelle Bewohnerverhalten ausforschen und die Wohnung aufgrund zweifelhafter Prämissen weiter „optimieren", einerseits zu Gunsten der Energiebilanz, andererseits zu Gunsten kommerzieller Gewinnmaximierung. Paternalismus ist per se problematisch, einer unter der Regie privater Unternehmen umso mehr.

Abschließende Bemerkungen

Hinsichtlich der Autonomie der Benutzer kann Hausautomatisierung in zwei Varianten vorkommen. Sie kann die Autonomie des Menschen stärken, indem sie ihm zusätzliche Kontrolle über sein Haus ermöglicht, sowohl durch Fernzugriff mittels mobiler ICT-Geräte als auch durch Festlegung von Regeln durch den Benutzer, bei denen der ausführende Computer eine dienende Rolle spielt. Mittel- bis langfristig werden voraussichtlich aber jene Systeme zunehmen, die vorerst eher in manchen Musterhäusern anzutreffen sind, bei denen Computer derart viele Entscheidungen treffen, dass die Autonomie der Bewohners geringer ist im Vergleich zu einem nicht automatisierten Haus. Viele der aktuell verfügbaren Systeme gehören noch zu ersterer Variante. Es ist eine paradoxe Entwicklung abzusehen, dass ein Trend zur Hausautomatisierung eingeleitet wird, indem einige „Pioniere" sich dafür entscheiden, weil sie ihnen unter anderem mehr Autonomie bringt, dass dann aber die langfristige Entwicklung in die umgekehrte Richtung führt. Über die Akzeptabilität dieser Autonomie-Einschränkung ist ein gesellschaftlicher Diskurs notwendig.

References

(Abrufdatum bei allen Internetquellen: 26. November 2014)

BITKOM (Bundesverband Informationswirtschaft, Telekommunikation und neue Medien): Heimvernetzung als Bindeglied zwischen Verbraucher und gesamtwirtschaftlichen Herausforderungen, 2012, http://www.bitkom.org/files/documents/Studie_I_Heimvernetzung_2012_I_WEB_Version%281%29.pdf

Borchers, Detlev: Home, sweet smart Home, 03.09.2012, http://heise.de/-1697773

Capurro, Rafael: Leben im Informationszeitalter. Berlin, Akademie Verlag 1995.

Capurro, Rafael: Existenzontologie: Operari sequitur esse. Zur existenzial-ontologischen Begründung der Netzethik, in: Hausmaninger Thomas / Capurro, Rafael (Hg.): Netzethik. Grundlegungsfragen der Internetethik, Schriftenreihe des ICIE Bd. 1. München, Wilhelm Fink Verlag 2002. 61-77. Im Internet: http://www.capurro.de/operari.html

Gigaset elements: Alles Gute zum Weltfrauentag!, 07.03.2014, https://www.gigaset-elements.com/de/blog/weltfrauentag/

Home Connect: FAQs zu Home Connect, http://www.home-connect.com/de-de/faq/faq.html#2

Home Connect: Nutzungsbedingungen für das Home Connect System, http://www.home-connect.com/de-de/nutzungsbedingungen/nutzungsbedingungen.html

Landeskriminalamt Nordrhein-Westfalen: Smart Home und Connected Home. Empfehlungen zur Sicherung digitaler Haustechnik (Stand August 2014), http://www.polizei.nrw.de/media/Dokumente/Behoerden/LKA/140811_LKA_SmartHome_Empfehlungen.pdf

Mims, Christopher: Das vernetzte Haus verkompliziert nur das Leben, 07.07.2014, http://www.welt.de/wallstreet-journal/article129882585/Das-vernetzte-Haus-verkompliziert-nur-das-Leben.html

Smart Automation: Home Automation, http://www.smartautomation.in/solutions/home-automation/

Sperlich, Kristine / Oehme, Ines (Umweltbundesamt): Schaffung einer Informationsgrundlage und Entwicklung von Strategien gegen "geplante Obsoleszenz". Fachgespräch bei der Bundestagsfraktion Bündnis 90 / Die Grünen am 20.03.2013 im Deutschen Bundestag, http://www.gruene-bundestag.de/fileadmin/media/gruenebundestag_de/themen_az/umwelt/PDF/UBA.PDF

Swisscom: Allgemeine Geschäftsbedingungen Interactive Home Services von Swisscom, https://sso.quing.com/quing/fileadmin/user_upload/pdf/agb_de.pdf

Weiser, Mark: The Computer for the 21st Century. Scientific American 265 (3) 1991, 66-75.

Weiser, Mark / Brown, John Seely: The coming age of calm technology. October 5, 1996, http://www.ubiq.com/hypertext/weiser/acmfuture2endnote.htm

Wiegerling, Klaus: Philosophie intelligenter Welten. München, Wilhelm Fink Verlag 2011.

Burkhard Schafer:

D-waste: Data disposal as challenge for waste management in the Internet of Things

Abstract:

Proliferation of data processing and data storage devices in the Internet of Things poses significant privacy risks. At the same time, faster and faster use-cycles and obsolescence of devices with electronic components causes environmental problems. Some of the solutions to the environmental challenges of e-waste include mandatory recycling schemes as well as informal second hand markets. However, the data security and privacy implications of these green policies are as yet badly understood. This paper argues that based on the experience with second hand markets in desktop computers, it is very likely that data that was legitimately collected under the household exception of the Data Protection Directive will "leak" into public spheres. Operators of large recycling schemes may find themselves inadvertently and unknowingly to be data controller for the purpose of Data Protection law, private resale of electronic devices can expose the prior owner to significant privacy risks.

Agenda:

Author:

Prof. Burkhard Schafer:

- University of Edinburgh, SCRIPT Centre, School of Law
- ☎ + 44 - 131 - 65 02 03 5 , ✉ b.schafer@ed.ac.uk, 💻 http://www.law.ed.ac.uk/people/burkhardschafer
- Relevant publications:
  - with Judith Rauhofer, Zbigniew Kwecka, William Buchanan, '"I am Spartacus" : privacy enhancing technologies, collaborative obfuscation and privacy as a public good' (2014) Artificial Intelligence and Law vol 22 p113-139.
  - with Wiebke Abel 'Guter Ork, Böser Ork: Snowden und die staatliche Überwachung von Online-Spielen in Grossbritannien' (2014) Jusletter-IT Vol 6 RZ 1-43 Vl 6.

ISSN 1614-1687

In the digital world, preventing others from acquiring information about us is just as difficult as to rid ourselves of data that we do not needed any longer. There might now be a recognised right to be forgotten, but our ability to "forget", especially for ordinary users of technology without specialist training, could turn out to be more limited than anticipated. Experts in computer forensics know just how difficult it is to delete information so that it cannot be reconstructed and retrieved again.[1] This raises particular challenges for the Internet of Things – when I resell my car or my fridge, or when I bring my washing machine to a recycling point, can I make sure that I do not leave data on them behind that could potentially tell others more about me than I am comfortable with?

Environmental vs Data Protection: setting out the conflict

With the proliferation of sensors, communication and data storage devises in the Internet of Things, concerns about privacy have increasingly come to the fore. In this new world, your car knows potentially more about you than your parents or partner - where exactly you travelled to last night, for instance, and maybe even if you were alone or the second seat was adjusted by someone.[2] In this future your fridge potentially talks to your toilet about providing a healthier diet for you, resulting in sensitive personal data that is collected, stored and exchanged in unprecedented quantities.[3] The debate on privacy in this interconnected world has created a lively academic debate.[4] In these discussions, the focus however is exclusively on the acquisition, use and storage of data while the equipment is in actual use and fully functional. This is not an unreasonable focus. After all, it is at this stage that very often a third party will be involved. To "know" where it is, my car has to communicate with an internet based service that provides this information, and the medical toilet will typically come as part of an integrated care home solution that also communicates with a care home provider or medical professional. The danger for the user of these devises then is abuse of this data by third parties, either through actions by that service provider directly (e.g. by reselling personal information) or through actions of others, be it criminals who succeed in compromising the security of my service provider, or by law enforcement agencies that acquire the data legally as part of an investigative process. Data acquisition and storage during the working life of an intelligent device undoubtedly covers the most important part of the life-cycle of electronic equipment, but nonetheless not all of it. Less prominent in the public awareness, and much less intensively discussed, is the destiny of the data once a device has reached the end of its working life, or at least the end of its usefulness for the current owner.

This aspect of secure data storage and disposal interacts in problematic ways with other societal costs of ubiquitous digital devices. While we often treat communication technology as mere abstract flow of data, we must not lose sight of the physical substratum that enables the exchange of data, the hardware that we use and more importantly, discard in ever-shorter cycles of consumption.[5] The global environmental problems that are created when the technology available to safely dispose of discarded equipment is outpaced by technological innovation of the gadgets themselves were recently the topic of a special issue of the International Review of Information Ethics[6]. Electronic waste or e-waste is increasingly recognised as an environmental problem in

1 See for an example Thing and Tan 2012

2 On privacy and autonomous vehicles in general see e.g. Glancy 2012

3 See for one vision of this specific smart device Schlebusch et al. 2014

4 See for an overview of the debate e.g. Weber, 2010; Medaglia and Serbanati 2010.

5 See for an empirical study e.g. Environmental Protection Agency (EPA) 2008

6 See Feilhauer et al. 2009

developed and developing countries,[7] with the latter often the recipient of waste from the former.[8] One important strategy to minimise the problem of e-waste is to prolong the consumption life cycle of electronic goods.

Following Lessig's concept of four distinct modes of regulation for the information society, we can distinguish between legal, market based and technological approaches to this problem. Prominent regulatory approaches are mandatory take-back and/or recycling schemes. From the 1990s onward, the "end of life challenge" – how can we safely dispose the ever increasing numbers of obsolete electronic products that contained significant quantities of hazardous materials - led the European Union to adopt the principle of "Extended Producer Responsibility" (EPR).[9] EPR makes manufacturers responsible for the full costs of their products across their lifecycle, thus internalising costs that are otherwise negative externalities. A typical way to achieve this are take-back obligations for their products once they reach the end of their useful lives. This can be combined with mandatory recycling schemes and targets for recycling.[10] Regulatory schemes like these create incentives for manufacturers to build equipment in a way that it reduces the costs of recycling, and/or by extending the life cycle of their products by design. Regulation by design is the second mode of regulation in Lessig's scheme. Finally, there are purely market based solutions. A flourishing second hand market in particular can extend the life cycle of goods that are abandoned by their owners not so much because they stop working properly, but because of social pressure, considerations of status and fashion.[11]

Reverse-logistics and mandatory take-back are at the heart of the Waste Electronic and Electrical Equipment (WEEE) directive (Directive 2002/96/EC) that established in Europe Extended Producer Responsibility.[12] While particularly rigorous in its demands, other countries are now slowly adopting similar approaches to the regulation of e-waste, though often with significant delays.[13]

At first sight, things look good, at least in Europe. We have an increasingly mature discussion about privacy concerns with regards to the Internet of Things. The upcoming Data Protection Regulation will enshrine the concept of Privacy by Design into law and substantially sharpen the responsibilities of data controllers. This will in particular also ensure better data protection in ubiquitous computing environments and the Internet of Things, where users will often be unaware of the fact that their personal data is gathered by their environment.[14] At the same time, we have a rigorous debate about the environmental impact of the hardware aspects of the IoT, in particular when it comes to e-waste. However, so far these two debates have not been linked with each other, and as we argue, this should be a cause for concern. If we increasingly resell, recycle or repurpose electronic devices, and if these devices increasingly store personal data about us, then the question arises how this data in turn can be safely disposed of. The aim of the WEEEE directive is to reduce hazardous waste, but "hazardous" is understood in terms of physically harmful substances only, the lead, cadmium or mercury that they contain, not the abstract and intangible information that they carry. Depending on the nature of the device, this information however can be potentially hazardous too, and in particular expose the previous

7 Babu, Anand, and Basha. 2007

8 See e.g. Wong, et al. 2007

9 Smith, 2009 p 9

10 Recycling targets need not be linked to EPR of course. It is also possible to require municipal authorities to organise and run recycling facilities. If these in turn are paid for by manufacturers proportionally to use, the same effects as EPR should ensue. "Free standing" mandatory recycling schemes where public entities rather than the manufacturer is legally and financially responsible have different effect on product design and manufacturer behaviour, but for our purpose, data security and privacy, pose the same issues

11 See e.g. Geyer and Blass V 2009 or Skerlos, et al 2003. Though under some conditions, second hand markets can also increase the demand for new goods, by reducing the costs of an upgrade. See e.g. Thomas, 2003.

12 Sachs,. 2006

13 Ongondo, Williams, and Cherrett. 2011

14 Kiss and Szőke 2015

owner to risks. Not only are the two debates not linked, at least in part, they are pursuing opposite goals. From a data protection perspective, the safest way, and for many technologically unsophisticated users the only feasible one, is not to resell their gadgets or give them to a recycle centre for refurbishing or other forms of reuse, but to put a hammer to the storage device and physically destroy it.[15] This can be in itself causing an environmental harm and it most certainly prevents extending the product's life cycle though reuse or resale. By contrast, resale or refurbishment are most likely to be successful if as much of the computational capability of the product is preserved, functional software should potentially be left on the device and only personal data should be deleted.

The conflict between the two objectives comes into even starker relief when we look at digital object memories, software objects intentionally designed to record the "life experience" of an object. Research has shown that such digital memories can increase the resale value of second hand electronic goods. Research in the Tales of Things and Electronic Memory (TOTeM) project approached the Internet of Things from this very perspective. It notes that our habit to surround ourselves with mementoes, objects with very strong personal resonance, faced in the past the problem that passage of time or change of ownership can mean that the stories behind this emotional meaning can get lost to future generations.[16] With digital memories associated with these objects, this danger decreases.[17] This has obvious implications for the second hand market, especially collectors. For obvious reasons, if I plan to sell the silver knife that was passed on through generations in my family, being able to demonstrate that it was given to my ancestor by Wellington at the Battle of Waterloo as a replacement for the dagger he threw to protect the general's life will increase its value immeasurably. Pierce and Paulos were amongst the first to identify the potential of digital memories for what they call "reacquisition and dispossession",[18] the sale and acquisition of second hand goods in charity shops or antique fairs. They proposed to enhance reacquisition practices explicitly with a focus on sustainable consumption, suggesting to digitally record the "histories of possession, maintenance and repair" of everyday objects. The TOTeM project developed these ideas further, showing how digital memories can enhance resale value.[19]

Quantifying the problem

We now have developed the broad setting for our discussion: from the perspective of environmental protection, we should increase resale, refurbishment, reuse and repurposing of electronic devices, including internet enabled devices in the IoT. For this, they need to reserve as much of other functionality has possible, and may even benefit from "added" information that tracks their history. From a Data Protection perspective, data minimisation and secure storage requirements should make us hesitant to give possession of any of these devices to third parties, even at their end of (for us) useful life. As noted above, there is at the moment a dearth of empirical studies on "information leakage" from second hand IoT devices. However, the related problem of security risks created by second-hand PCs has received attention for some time now.

15 Physical destruction of hard drives is often recommended for particularly sensitive information when disposing of compute equipment. See e.g. http://abouthipaa.com/wp-content/uploads/NIST-Special-Publication-800-88_Guidelines-for-Media-Sanitization_SP800-88_rev1.pdf. The methods mentioned there are all environmentally hazardous and require specialist skills.

16 Barthel, et al. 2013

17 Bell and Gemmell, 2009

18 Pierce, and Paulos. 2011

19 de Jode, et al. 2012.

Even with traditional computers, privacy conscious recycling is a concern. The problem of data remanence in "automated information systems" was identified first by the US military in the 1960s.[20] In the 1980s, the National Security Agency became responsible for computer security within the Department of Defense and commissioned a series of studies at the Illinois Institute of Technology, and Carnegie-Mellon University to evaluate the efficiency of secure data sanitization such as degaussing, physical destruction and various forms of overwriting. While the security culture of the military and the technical infrastructure available to them thus ensured that their computers were safely prepared for reuse, neither their level of awareness, nor their technical abilities, found a counterpart in the civilian sector. There, anecdotal stories of inadvertent data disclosure through reselling, donating or otherwise discarding of personal and company computer abound. In 1997, a resident of Nevada bought a used IBM computer and discovered that it contained the prescription records of 2,000 patients, including their names, addresses and Social Security numbers, a list of the medication they had been prescribed (some for alcoholism and depression). The computer could be traced back to a pharmacy that had sold it when updating their computer system. In 2001, a US company auctioned off more than 100 computers which confidential client information. In 2002, a United States Veterans Administration Medical Center in Indianapolis discarded over 100 computers, donating some to schools while selling others. Some ended up in second hand shops where a journalist bought one, only to find that the computer contained highly sensitive medical information, including the names of veterans with AIDS and mental health issues. In addition to the medical data, credit card information was also stored on the device and easily recoverable.[21] Subsequent systematic studies confirmed again and again this picture. Back in 2000, Garfinkel and Shelat bought 158 hard drives on the secondary from a variety of sources, specialist second hand computer retailers to small companies selling directly their own surplus equipment. Many of the purchases were done through ebay. Even from this small sample, they were able to retrieve thousands of credit card details, significant amounts of personal and business emails and letters and also medical data.[22]

While Garfinkel and Shelat thought in 2003 that wider awareness of privacy risks in second hand computer markets would quickly reduce this problem, subsequent studies very consistently find the same problem reoccurring, independent of the details of the data storage technology, the sector (medical service providers continue to figure prominently event though privacy awareness in general has risen dramatically in that profession), country or age group.[23]

On the basis of this research, we can make an *a fortiori* argument: Data stored on personal computers is highly conspicuous – we know it is there because in most cases, we had to add it directly and explicitly. Personal computers are easily identifiable through their visual design. Slightly more difficult, but still relatively easy, is to identify their data storage component. Furthermore, physical removal of the hard drive is in many cases unnecessary, as user-friendly tools such as CCcleaner and other anti-forensic software allow secure data overwrite even to unsophisticated users. Despite this relative ease to prepare a personal computer for resale in a privacy preserving way, we find again and again that individual users, but also larger organisations, fail to take the necessary steps. In the IoT, none of these advantages are present: Data will often be collected without explicit user input, the diversity of smart devices makes it impossible to say just from visual inspection if an object is storing or processing data, and if so which type of data (one can think e.g. of smart clothing and jewellery). The precise space where data is stored will often be difficult to access (e.g. in a fridge or a central heating system) and they will not normally run software that allows easy data deletion.

20 National Computer Security Center, "A Guide to Under- standing Dataremanence in Automated Information Sys- tems," Library No. 5-236,082, 1991 http://fas.org/irp/nsa/rainbow/tg025-2.htm

21 all three cited in Garfinkel, and Shelat 2003 p.17-18

22 ibid p. 24-26

23 see e.g. El Emam, Neri, and Jonker 2007; Jones, Valli, and Dabibi. 2010;.Szewczyk. 2011; Lim et al 2014

Mitigation Strategies

What can we do to reduce the inherent risk for data security that recycling smart electronic goods in the IoT brings, while maintaining the benefits of mandatory take-back schemes and strong second hand market in electronic goods?

First, there are legal issues to consider. On the one hand, discarded data has to be recognised as an issue for the purpose of data protection law, while at the same time we must be careful not to overburden recycling providers or small second-hand retailers. In some jurisdictions, data discarded by its owner loses all legal protection. In the US, *California v. Greenwood* ensures that data on discarded devices do not enjoy a reasonable expectation of privacy. The discussion above should have made it clear how problematic this precedent is when applied to smart devices in the IoT. In addition, it also highlights a problem that European based recycling companies will face if they aim to transport the discarded good to other countries for refurbishment – inadvertently they may in the process transfer personal data outside the protection of EU law. In Europe, the legal situation is not quite as dire. Especially when customers are de facto forced to use a recycling service as the only lawful means (under environmental law) to discard used electronic equipment, the resulting power imbalance will be recognised by the new Data Protection Regulation. This means in particular that discarding a device in this way will not be constructed as implied (or possibly even explicit) consent to allow unfettered use of that data by third parties. Conversely, EU data protection law in interaction with the WEEE Directive also offers some protection for the organiser of recycling schemes: While they become data processors, or possibly in some set-ups even data controllers, the WEEE Directive provides a legal ground for the processing of the data. However, this privileges possibly unduly recycling operators set up to fulfil EPR duties of manufacturers over those who organise recycling schemes out of altruistic environmental or social concerns. Accessing data for the sole purpose to delete it as part of a recycling or resale/refurbishment scheme should therefore always be considered as a "legitimate interest".

This still creates burdens on operators of recycling schemes or second hand retailers, and also leaves risks for users. This burden can be minimised to a degree through design choices – ideally, the data storage component should be easily accessible, the data storage unit easily removable, and user data and other software stored separately. This should prevent the need to destroy equipment just to erase personal data, as discussed above. Easy ways to effect a "factory reset" that deletes all user data, while not as secure as using scrubbing software, would be highly desirable. "Privacy by design" is likely to be explicitly mentioned in the new Data Protection Regulation. Here Data protection law can learn from environmental law and ensure that "privacy by design" covers not just the operation of a device, but also the "D-waste" at the end of the lifecycle of a device. In the long run, the problems outlines above may require rethinking the "household exception" of Data Protection law. Given the complexity of compliance with DP law, it is on the one hand very reasonable to exempt data that is collected and processed in a purely domestic setting, e.g. my address list on my mobile phone. Much of the data in smart devices will be of that nature. But as our discussion shows, sound environmental principles make it inevitable that few devices will stay forever within the confines of just one household. That often the data is the data of the owner of a device only, or data of others collected lawfully under the household exemption, should not mean that we cannot think of reasonable safeguards when the data is discarded. A mandatory labelling scheme for smart devices that uses a traffic light warning system could for instance help the owner of a device to carry out an informal privacy risk assessment (make informed choices) when preparing a device for private resale or for return to a recycling scheme.

References

Dong, Tao. "Design Consideration of a Health-Information-Technology-Supported Intelligent Urinalysis System." In Advanced Materials Research, vol. 989, pp. 1077-1081. 2014.

Thing, Vrizlynn LL, and Darell JJ Tan. "Symbian smartphone forensics and security: Recovery of privacy-protected deleted data." Information and Communications Security. Springer Berlin Heidelberg, 2012. 240-251

Feilhauer, Matthias, et al. "Ethics of waste in the information society." special issue of International Review of Information Ethics 11 (2009)

Glancy, Dorothy J. "Privacy in Autonomous Vehicles." Santa Clara L. Rev. 52 (2012): 1171

Schlebusch, Thomas, et al. "Unobtrusive and comprehensive health screening using an intelligent toilet system." Biomedical Engineering/Biomedizinische Technik (2014). DOI: 10.1515/bmt-2013-0140, October 2014

Weber, Rolf H. "Internet of Things–New security and privacy challenges." Computer Law & Security Review 26.1 (2010): 23-30

Medaglia, Carlo Maria, and Alexandru Serbanati. "An overview of privacy and security issues in the internet of things." In The Internet of Things, pp. 389-395. Springer New York, 2010

Wong, M. H., et al. "Export of toxic chemicals–a review of the case of uncontrolled electronic-waste recycling." Environmental Pollution 149.2 (2007): 131-140

Babu, Balakrishnan Ramesh, Anand Kuber Parande, and Chiya Ahmed Basha. "Electrical and electronic waste: a global environmental problem." Waste Management & Research 25.4 (2007): 307-318

Thomas, Valerie M. "Demand and Dematerialization Impacts of Second-Hand Markets." Journal of Industrial Ecology 7.2 (2003): 65-78

Geyer R, Doctori Blass V (2009) The economics of cell phone reuse and recycling. Int J Adv Manuf Technol 47(5-8):515- 520

Skerlos SJ, Morrow WR, Chan KY, Zhao F, Hula A, Seliger G, Basdere B, Prasitnarit A (2003) Economic and Environmental Characteristics of Global Cellular Telephone Remanufacturing. In: IEEE InternationalSymposiumon Electronics and the Environment, 2003, 99–104. IEEE. http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=1208055

Sachs, Noah. "Planning the funeral at the birth: Extended producer responsibility in the European Union and the United States." Harv. Envtl. L. Rev. 30 (2006): 51

Ongondo, Francis O., Ian D. Williams, and Tom J. Cherrett. "How are WEEE doing? A global review of the management of electrical and electronic wastes." Waste management 31.4 (2011): 714-730

Kiss, Attila, and Gergely László Szőke. "Evolution or Revolution? Steps Forward to a New Generation of Data Protection Regulation." Reforming European Data Protection Law. Springer Netherlands, 2015. 311-331

Barthel, Ralph, et al. "An internet of old things as an augmented memory system." Personal and ubiquitous computing 17.2 (2013): 321-333

Pierce, James, and Eric Paulos. "Second-hand interactions: investigating reacquisition and dispossession practices around domestic objects." Proceedings of the SIGCHI Conference on Human Factors in Computing Systems. ACM, 2011

de Jode, Martin, et al. "Enhancing the'second-hand'retail experience with digital object memories." Proceedings of the 2012 ACM Conference on Ubiquitous Computing. ACM, 2012

Smith, Ted. "Why we are „Challenging the Chip ": The Challenges of Sustainability in Electronics." International Revie of Information Ethics11 (2009): 9.

Garfinkel, Simson L., and Abhi Shelat. "Remembrance of data passed: A study of disk sanitization practices." IEEE Security & Privacy 1.1 (2003): 17-27.

El Emam, Khaled, Emilio Neri, and Elizabeth Jonker. "An evaluation of personal health information remnants in second-hand personal computer disk drives." Journal of medical Internet research 9.3 (2007)

Szewczyk, Patryk. "Analysis of Data Remaining on Second Hand ADSL Routers." Journal of Digital Forensics, Security and Law 6.3 (2011): 17-30.

Jones, Andy, Craig Valli, and G. Dabibi. "The 2009 Analysis of Information Remaining on USB Storage Devices Offered for Sale on the Second Hand Market." 7 th Australian Digital Forensics Conference. 2009.

Lim, Charles, Ivan Firdausi, and Andry Bresnev. "Forensics Analysis of Corporate and Personal Information Remaining on Hard Disk Drives Sold on the Secondhand Market in Indonesia." Advanced Science Letters 20.2 (2014): 522-525.