Project Deliverable

Project Number:	Project Acronym:	Project Title:
287901	BUTLER	uBiquitous, secUreinTernet-of-things with Location and contEx-awaReness

Instrument:	Thematic Priority
Integrated Project	Internet of things

Title

Ethics, Privacy and Data Protection in BUTLER

Contractual Delivery Date:	Actual Delivery Date:
May 2013	July 2013

Start date of project:	Duration:
October, 1st 2011	36 months

Organization name of lead contractor for this deliverable:	Document version:
SWC	V1.2

Dissemination level (Project co-funded by the European Commission within the Seventh Framework Programme)		
PU	Public	**X**
PP	Restricted to other programme participants (including the Commission	
RE	Restricted to a group defined by the consortium (including the Commission)	
CO	Confidential, only for members of the consortium (including the Commission)	

Authors (organizations) :

Katharina LIEBRAND (SWC), Katja MOSER (SWC), Severine KNÜSLI (SWC),Bertrand COPIGNEAUX (Inno), Franck LE GALL (inno), Phillippe SMADJA (GTO), Alexey ANDRUSHEVICH (iHomeLab), Foued MELAKESSOU(University of Luxemburg).

Reviewers (organizations) :

Maria Fernanda SALAZAR (ERC).

Abstract :

This document is an intermediate contribution of the BUTLER project activities on the socio-economical impact of the Internet of Things (Work Package 1 and 6 activities), as requested during the Year 1 review conducted in October 2012.

This document deals specifically with the ethical questions encountered within typical Internet of Things scenarios and contains an outline of the issues to be solved, if Internet of Things is to be successful in the market.

The document gathers results from the following main sources:

- Customer Insight Interviews conducted in several European countries by the BUTLER consortium partners with the specific goal to collect input on end user needs and expectations towards the Internet of Things
- Consolidated results from several workshop sessions having been held for example at IoT Week in Venice (June 2012) or the IoT Ethics session introducing the BUTLER Plenary In Luxemburg (September 2012)
- Results and reports from other – mainly European – research projects and IoT conferences
- Insight gathered from market reviews and other sources during the work on work package 1 and 6 of BUTLER

The content of this document is part of the overall deliverable D1.3, which will be available at the end of the BUTLER project in autumn 2014.

Keywords :

Ethical issues, privacy, data protection, customer expectations, requirements.

Disclaimer

Revision History

The following table describes the main changes done in the document since it was created.

Revision	Date	Description	Author (Organisation)
V0.1	January 2013	Document creation and first Table of Content	Bertrand COPIGNEAUX (inno)
V0.1.2	January 2013	Updated ToC based on SWC inputs	Bertrand COPIGNEAUX (inno)
V0.1.5	January 2013	Updated TOC based on Conf Call discussion	Katja MOSER, Katharina LIEBRAND (SWC)
V0.2	March 2013	Completed of the SWC chapters	Katharina LIEBRAND, Katja MOSER (SWC)
V0.3	March 2013	Completed Chapters 5.2 &6.3	Phillippe SMADJA (GTO)
V0.4	April 2013	Completed sections	Katharina LIEBRAND, Katja MOSER (SWC)
V0.5	19 April 2013	Further sections completed	Katharina LIEBRAND (SWC)
V0.6	29 April 2013	Further sections completed	Katharina LIEBRAND (SWC)
V0.7	20 May 2013	5.1.4; 5.1.5 ; Further sections completed	Katharina LIEBRAND (SWC)
V0.8	22 May 2013	Chapter 3: completed	Bertrand COPIGNEAUX (inno)
V0.9	May 2013	Chapter 4.4.3 Legal Overview and Current Situation on Privacy	Severine KNÜSLI(SWC)
V0.9.1	May 2013	Contribution on Chapter 7 based on Deliverable 1.2	Alexey ANDRUSHEVICH (iHL)
V1.0	May 2013	Finalization of all sections and document	Bertrand COPIGNEAUX (inno)
V1.1	June 2013	Document review	Maria Fernanda SALAZAR (ERC)
V1.2	June 2013	Finalization and final review	Franck LE GALL (inno)

Table of Content

1. Acronyms and Definitions

1.1. Acronyms

Acronyms	Definition
6LoWPAN	IPv6 over Low power Wireless Personal Area Networks.
AAL	Assisted Ambient Living
AS	Authorization Server
CCTV	Closed Chanel Television
COAP	Constrained Application Protocol
CVO	Composite Virtual Object (iCore)
DG Connect	Directorate General for Communication Networks, Content and Technology of the European Commission
DOW	Description of Work (of the BUTLER Project)
DPA	Data Protection Authority
DPO	Data Protection Officer
ECHR	European Convention of Human Rights
ECtHR	European Court of Human Rights
EFTA	European Free Trade Association
EU	European Union
FTA	Federal Trade Commission (USA)
GBA	Generic Bootstrapping Architecture
GDPR	General Data Protection Regulation
GSM	Global System for Mobile Communications
HMI	Human Machine Interface
HSM	Hardware Security Module
iCore	iCore, FP7 European Project
ICT	Information and Communication Technologies
ID	Identification
IEEE	Institute of Electrical and Electronics Engineers
IERC	Internet European Research Cluster
IoT	Internet of Things
IOT-A	Internet of Things Architecture, FP7 European Project
IP	Internet Protocol
IPR	Intellectual Property Rights
IT	Information Technologies
MEESTAR	Model for advantages, disadvantages and social / economical impact
NFR	Non Functional Requirement
OAUTH	Open standard for authorization
OECD	Organization for Economic Cooperation and Development
PCI	Payment Card Industry
PET	Privacy Enabling Technologies
PIA	Privacy Impact Analysis
PII	Personally Identifiable Information
PIN	Personal Identification Number
PTSD	Post Traumatic Stress Disorder

RFID	Radio Frequency Identification
RSA	Ron Rivest, Adi Shamir and Leonard Adleman Cryptography Algorithm
SMS	Short Message Services
SSL	Secure Socket Layer
TLS	Transport Security Layer
UC	Use Case
UCLA	University of California, Los Angeles
UK	United Kingdom
VO	Virtual Object (iCore)
ZIP Code	Zone Improvement Plan

2. Executive Summary

This document is an intermediate contribution of the BUTLER project activities on the socio-economical impact of the Internet of Things (Work Package 1 and 6 activities), as requested during the Year 1 review conducted in October 2012. It deals specifically with the ethical questions encountered within typical Internet of Things scenarios and contains an outline of the issues to be solved, if Internet of Things is to be successful in the market.

The document starts by presenting the motivation behind this deliverable: based on the acknowledgement that Ethics, Privacy and Data security issues exist in IoT and that they can have a strong impact on the deployment of these new technologies, the BUTLER project has been, since its start strongly involved in the study of these issues. This deliverable will provide a first unified view on the activities of BUTLER in the Ethics, Privacy and Data Protection aspects of IoT.

We then present an analysis of the expressed needs, requirements and expectations of data protection, privacy, and ethical behaviours in Internet of Things use cases. The analysis starts by tentative definitions of ethical behaviour and privacy and of the main issues in the field of the Internet of Things. This includes “classical” risks link to handling personal information such as privacy breaches, ownership and repurposing of data, as well as more in depth issues linked to the eventual wide spread deployment of IoT such as the risk of social and knowledge divide, loss of autonomy, and increased need for continuity and availability of services. These issues are then further analyzed based on the activities of the BUTLER project: in the analysis of requirements done by the project partners, in the perception of the general public, and through consultation with external experts and other research projects.

In section 5 we present the state of the art in term of privacy and data protection solutions for Internet of Things use cases and applications. We review general principles of privacy such as the need of informed consent, the principles of minimal disclosure, and anonymization of data, and the MEESTAR (**M**odell zur**e**thischen**E**valuation **s**ozio-**t**echnischer **Ar**rangements) model. We then present rapidly the main data protection techniques which are presented in more detail in BUTLER deliverable 2.1[1]

Based on the expectations identified in section 4 and on the state of the art done in section 5, we propose different approaches to handle privacy and data protection issues in Internet of Things use cases. The approach proposed are broad and complementary: from the commitment to general principles for data protection, the privacy by design approach, the set up of technical solutions, and the important need for communication on privacy and data protection.

Finally, we present the activities and policy followed by the BUTLER consortium in the project experimentations (proof of concepts and field trials) regarding privacy, security and data protection. The main principles and legislation followed are presented, as well as the technical data protection mechanisms and the actual process used for protecting end users in Field Trials.

[1] BUTLER Deliverable 2.1 : requirements, specifications and security technologies for IoT Complex Aware Applications available on http://www.iot-butler.eu/download/deliverables

3. Document Motivations

In this section we present the motivation behind this deliverable: based on the acknowledgement that Ethics, Privacy and Data security issues exist in IoT and that they can have a strong impact on the deployment of these new technologies, the BUTLER project has been, since its start strongly involved in the study of these issues. This deliverable will provide a first unified view on the activities of BUTLER in the Ethics, Privacy and Data Protection aspects of IoT.

3.1. Ethics, Privacy and BUTLER

3.1.1. Identified Ethics and Privacy Issues

3.1.1.1. Privacy

The goal of the project BUTLER –as stated in the DOW- is an ubiquitous, secure internet-of-things with location and context awareness. Thus the main challenges from a user/service perspective relate to:

- pervasiveness (uniformity of performance anytime and anywhere)
- awareness (inversely proportional to the degree of knowledge required from users)

In short BUTLER aims at a system where network reactions to users are adjusted to their needs (learned and monitored in real time). The main ethical issues then seem to be, how to guarantee:

- the security of the data stored (or mined) to support the BUTLER services
- the privacy of the user

Of these two issues

- Data Security is more of a technical problem, and while no doubt difficult to achieve, it does not raise deeper ethical questions
- Privacy on the other hand is undoubtedly also an ethical issue

Privacy is generally seen to be best protected, if these parts of a privacy framework are put into place

- Ensuring the gathering of the user consent
- Implementation of the minimal disclosure principle, whereby each actor in the information chains has solely access to the data needed to deliver the service
- Or alternatively anonymization of data, if data is released to third parties, to protect the identification of the data subject

In fact most countries have legislation in place to ensure these minimal standards are being adhered to and so far in most environments these rules seem to have been sufficient.

3.1.1.2. Other Possible Ethical Issues

From the discussions about some of the individual vertical scenarios which may be covered by an IOT application some more ethical questions can be derived, which usually centre around these subjects

Panopticon or Surveillance Society:

The panopticon is originally a prison designed by Jeremy Bentham, where the guards are placed in a structure in the middle of a circular prison, thus being able to observe everything the inmates did, while not being seen themselves.

Bentham himself described the panopticon as "*a new mode of obtaining power of mind over mind, in a quantity hitherto without example*."

The psychological foundation behind the panopticon is that people do behave differently if they think they're being watched. Thus constant surveillance is severely limiting personal freedom.

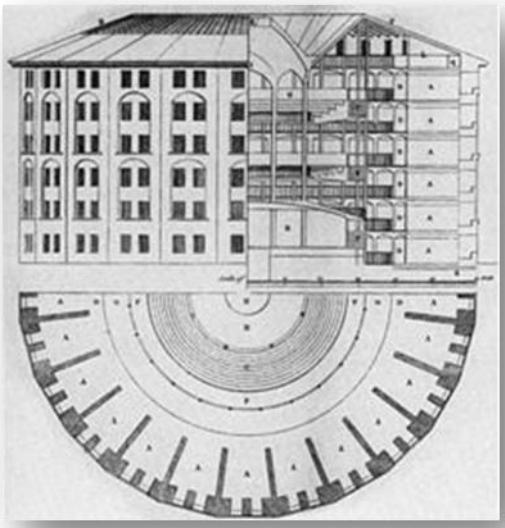


Figure 1: Plan of Bentham's Panopticon (Source Wikipedia)

There is a certain concern that the IoT with its increased ability to monitor and record almost all aspects of people`s lives will have a similar effect on society as the panopticon was supposed to have on the prison inmates.

3.1.1.3. Lack of Autonomy and Self Determination

Closely related to the idea of the surveillance society is the loss of autonomy or self determination. These concerns are usually raised in conjunction with the Health Care vertical, especially with systems for Assisted Ambient Living (AAL).

The MEESTAR model described in chapter 5.1.5 for example is very much concerned with these kinds of ethical questions.

3.1.1.4. Isolation and Loss of Interpersonal Contact

In the customer surveys we conducted as part of BUTLER almost 50% of interviewees where concerned about the possibility that IoT applications might lead to greater isolation and loss of contact with other human beings. On the other hand, the perception of what is an "interpersonal contact" might be evolving with the technology (and their use and acceptance), as new generations and extensive users of novel ICT technologies seem to show that "virtual" contact can still have social benefits[2].

3.1.2. Potential Impact

As the concepts and technologies behind IoT are relatively new, until recently ethics and privacy issues had been mostly ignored by service provider, and treated only when concerns arose and threatened their business. However, with the numerous cases of privacy breaches observed in the

[2] "The Benefits of Facebook "Friends:" Social Capital and College Students' Use of Online Social Network Sites" Nicole B. Ellison, Charles Steinfield, Cliff Lampe, Journal of Computer-Mediated Communication July 2007. http://onlinelibrary.wiley.com/doi/10.1111/j.1083-6101.2007.00367.x/full
See also: Zur, O. & Zur, A. (2011): On Digital Immigrants and Digital Natives: How the Digital Divide Affects Families, Educational Institutions, and the Workplace. Zur Institute. http://www.zurinstitute.com/digital_divide.html

social network field, and the increased concerned on communicating object (observed for example with the crystallization of the public opinion on RFID technology) the general awareness has been raised to pay more attention to the data users are spreading around. The public true understanding of the issue remains low, but the mere rumours of a potential threat to privacy is often enough to damage business.

Already some example demonstrates the importance of the ethics and privacy issues such as the backlash on smart metering technologies. The recent events in the Netherlands (where the deployment of Smart Metering had to be made optional to respond to privacy concerns)[3] illustrate the initial lack of concern for the potential ethics and privacy issues transformed into a threat to the whole industry. The complexity of the technology involved in the new IoT services envisioned can lead to a general misperception of the potential threats to privacy of new technologies and services. This misperception can happen in one way (as a underestimation of the potential threat to privacy of new use cases) or in the opposite (as an unrestricted reject of a technology based on overestimated threats to privacy), both way being damaging for society as a whole.

However, if treated accordingly, the ethics and privacy issues transforms from a threat to an opportunity. Better understanding of the service by the user increase acceptance and create trust in the service. This trust becomes a competitive advantage for the service provider that can become a corner stone of his business model. In turn the economical interest of the service providers for ethics and privacy issues, derived from this competitive advantage, becomes a guarantee for the user that his privacy will be respected.

3.1.3. BUTLER activities

The BUTLER project, along with the other IoT projects involved in the IoT European Research Cluster has recognized these potential impacts and committed to address them. From even before the very start of the project, the consortium addressed the privacy concerns linked with the execution of the project in the Description of Work. In Section B4 of the Description the consortium described the ethics issues identified within the scope of the project:

- Collection of Human data / data collection: requesting and obtaining data.
- Privacy: collection and storage of data.
- Tracking the location and observation of people.

The Description of Work then lists the regulation to be followed by the project and answers in details to the questions listed in the "Data protection and privacy ethical guidelines"[4], version 5, edited by the European Commission on 18th September 2009.

The goal of the BUTLER project is the creation of an experimental technical platform to support the development of the Internet of Things. The main specificity of the BUTLER approach is its targeted "horizontality": The vision behind BUTLER is that of a ubiquitous Internet of Things, affecting several domains of our lives (health, energy, transports, cities, homes, shopping and business) all at once. The BUTLER platform must therefore be able to support different "Smart" domains, by providing them with communication, location and context awareness abilities, while guaranteeing their security and the privacy of the end users. The issue of security and privacy is therefore central in the BUTLER project and develops in several requirements; the project requirements (including those on privacy and security) have been documented in details in Deliverable 1.1 (and reminded here in Annex 1).

[3] http://vorige.nrc.nl/international/article2207260.ece/Smart_energy_meter_will_not_be_compulsory

[4] https://www.google.fr/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&ved=0CC4QFjAA&url=ftp%3A%2F%2Fftp.cordis.europa.eu%2Fpub%2Ffp7%2Fdocs%2Fprivacy.doc&ei=mNG-UZb8LfD64QSs3oCwAQ&usg=AFQjCNGoXTYM8MbKaGHkYhxHJYT88GliRA&sig2=_y1Sya7qhJqv1PqvWtYUmQ&bvm=bv.47883778,d.bGE

The main requirements relate to:

- Standard issues of data security, both at data storage level as at data communication level exists in IoT application. The diversity and multiplicity of the "things" connected by the internet of things, and the data exchanged further amplifies and complicate these requirements.
- The application enabled by the Internet of Things may pose additional privacy issues in the use that is made of the data. From the collection of data by the applications (which should be conditioned by an "informed consent" agreement from the user), to the profiling, exchange and sharing of these data necessary to enable true "context awareness".
- Finally as presented in the Ethics Factsheet[5] resulting from the expert group on IoT Ethics, the IoT applications also raise some other ethics challenges which have to be acknowledged and taken into account as requirements for the IoT platform.

The project addresses these requirements in two ways, running in parallel and equally important:

- By addressing the scientific issues and technological solutions to the issues of privacy and security. The project task 2.1 and 2.2 address the issue of "Trust, Privacy, and Security" at lower and upper layers. A first deliverable entirely focused on the enabling technologies available to address the privacy and security issues has been delivered by BUTLER after the first year of the project (Deliverable 2.1 Requirements, Specification and Security Technologies for IoT Context-aware network). The work on technical solutions to ensure privacy and security continues in the project as the enabling technologies described in deliverable 1.2 are now being implemented in the architecture and platform.
- By addressing the issues of privacy from a societal and business model point of view. This is covered by the work of Work Package 1 (Application Use Cases and Requirements for Pervasive Context-Awareness) and by task 6.3 (Exploitation and IPR Management). Over the first year of the project, in addition to the gathering of requirements (D1.1 described above), this track focused on the constitution of a specific sub-group of the project External Member Group involving Ethics and Privacy users and on the gathering of users' perspectives on IoT through detailed, open, end user interviewed.

These activities, both technical and business oriented on the potential security, privacy and ethics issues of IoT have been lead and will continue to be done in strong cooperation with the relevant research communities, through the production of papers, the involvement in conferences, and the active participation in the IoT European Research Cluster activity chain 5 "Governance, Privacy and Security issues".

[5] http://ec.europa.eu/digital-agenda/en/news/conclusions-internet-things-public-consultation

3.2. Document origins

The first review of the project confirmed the strong interest and needs for an Ethics and Privacy oriented vision of the IoT. As presented above, the BUTLER project has committed to address these issues and this work is being carried in different tasks, addressing the different aspects of the issue (technical and non technical), and monitored into different deliverable. However the reviewers encouraged us to unify and formalize our findings and activities in this field in a single report so they can best be monitored and most importantly reused and transferred to other projects and stakeholders of the IoT domain.

These discussions lead to the following formal request by the project reviewers:

> *The consortium should produce an extra report that **identifies and privacy and data protection issues** and **how these would be dealt with within the project** so that all members can share a common understanding. This would allow all concerns to be shared so that the consortium can together **develop a common position on how these issues are to be handled within BUTLER.** The reviewers suggested that the consortium develop the project's position on data protection topics and making sure that all participants (and possibly the whole cluster) share it.*
> *BUTLER has the scope to allow a significant number of privacy and data protection concerns in the IoT domain to be elicited or uncovered. The consortium is encouraged to **try and identify potential concerns including those that it may not yet have technological solutions** for or be able to tackle within the scope of BUTLER but which could be used to **raise awareness in the IoT domain** so that other projects or future research could address these.*
> *The extra report is to be produced within 6 months of the review meeting for review by the reviewers. The report should become **a living document to be updated regularly with new privacy or data protection concerns** as they are uncovered or come to light to the end of the project*

This deliverable will provide a first unified view on the activities of BUTLER in the Ethics, Privacy and Data Protection aspects of IoT. This view will be updated and incorporated in the larger deliverable 1.3 (schedule at the end of the project) on the socio-economic impact of IoT and the BUTLER project.

4. Ethics Expectations

In this section, we present an analysis of the expressed needs, requirements and expectations of data protection, privacy, and ethical behaviours in Internet of Things use cases. The analysis starts by tentative definitions of ethical behaviour and privacy and of the main issues in the field of the Internet of Things. These issues are then further analyzed based on the activities of the BUTLER project: in the analysis of requirements done by the project partners, in the perception of the general public, and through consultation with external experts and other projects.

4.1. Ethics, Privacy and the Internet of Things

4.1.1. A Short Definition of Ethical Issues

In general if people talk about ethical issues, their first tendency seems to be to concentrate on the "big" and controversial topics like slavery, abortion, euthanasia, torture or animal rights.

Looking at the Internet of Things with these kinds of issues in mind, it is not very obvious, why there should be any ethical issues in IoT at all.

Most of the definitions of ethics at first do not seem very helpful, either. Take this one by Adam Blatner[6] for example:

- Ethics involves the sphere of interpersonal, group, and community politics at the level of value
  - not just what can be achieved or how to achieve it,
  - but more what should be sought, in the realm of social harmony and fairness
- It is the complexity of the other side of individualism
  - other than taking care of oneself, what do we want our collective to do or refrain from doing?
- Ethics looks at our proper relations, our duties to each other, individually and collectively

Again, while the definition of ethics is clear and straightforward, the relationship to the IoT is not obvious. After all, the Internet of Things is not about human interaction, but mainly about interactions of machines with each other. So why should ethics be of concern?

Closer to the mark with regard to possible ethical issues with the Internet of Things seems this definition about business ethics[7]:

- Business ethics are standards businesses should observe in their dealings over and above compliance with the letter of the law.
- This covers questions such as fair dealing with their labour force, customers, suppliers, and competitors, and the impact of their activities on the environment, public health, and animal welfare.

After all, the Internet of Things is – or at least should be – foremost a business venture, a vehicle for companies to make money and bring value to customers. So within the context of the BUTLER project it makes sense to evaluate the possible controversial ethical topics within the IoT and compare the legal regulations with the expectations the future customers have about ethical issues

Regarding privacy, there are also lot of definitions and controversies about the Privacy Concept. There is lot of definitions with many drawbacks. In "Privacy and Freedom" - 1967 – Alan Westin defines privacy as "the claim of individuals, groups, or institutions to determine for themselves

[6] Adam Blatner, M.D. "**ETHICAL ISSUES IN CONTEMPORARY CULTURE", cited after** http://www.blatner.com/adam/psyntbk/ethicissues.htm

[7] John Black, NigarHashimzade, Gareth D. Myles "**A Dictionary of Economics",** Oxford University Press, 2009

when, how, and to what extent information about them is communicated to others", but as Jeff Jarvis said in – "Public Parts; How Sharing in the Digital Age Improves the Way We Work and Live" – 2011, it depends also on the way the information is retrieved. For instance if the information is retrieved in a public space (a photo on a street), is the photo public or private? Privacy is related to the notion of Personal Data. In the "Data Protection Directive 95/46/EC"[8] related to the protection of individuals with regard to the processing of personal data and on the free movement of such data, European Commission gives the following definition:

Personal Data "Any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity [art. 2(a)]".

From an ethic point of view, in an age of technologically enabled increased transparency and social interactions, and facing the technological possibility to make monitoring and surveillance ubiquitous, privacy remains a value to be safeguarded. First because privacy still is an important, even rising, concern of end users (see section 4.3 on end user perception). Secondly because protecting privacy at the individual level can be made compatible with an increased transparency at organisational level[9] or with the increased demand for security. And finally because protecting privacy is necessary to safeguard and enable innovation and critical thinking (recent studies[10] shows that fully transparent organizations hinder productivity and innovation).

4.1.2. Ethics and the IoT

Based on these initial definitions of ethics we can start to think on the potential impacts of IoT, what will the wide deployment of a horizontal IoT change in the realm of social harmony and fairness? And based on these potential impacts, what are the necessary implications for the companies and researchers involved in the development, deployment and commercialization of these new technologies and services?

Internet has dramatically changed the way we interact with information (personal, business, legal, health, etc.) and allowed reliable and rapid exchange of large amount of information between people without any distance restrictions. These transformations of our way of life gave rise to several ethical concerns in particular related to privacy and the sharing of personal information. The Internet of things extends and automates the information sharing features from humans to machines, machines that have not any ethical concerns as humans. Machines (e.g. sensors) can capture more and more information on users and their surrounding environments. Furthermore, the machines (e.g. actuators) have the power of modifying the physical environment of users. IoT adds therefore additional ethical questions such as the potential risks linked with the control of the "real world devices" by internet, or the ethical implication of a society where monitoring is ubiquitous.

[8] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML

[9] Transparent Government, Not Transparent Citizens https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/61279/transparency-and-privacy-review-annex-a.pdf

[10] The Transparency Paradox: A Role for Privacy in Organizational Learning and Operational Control, Ethan S. Bernstein Administrative Science Quarterly, June 2012. Available here: http://asq.sagepub.com/content/57/2/181.full.pdf+html

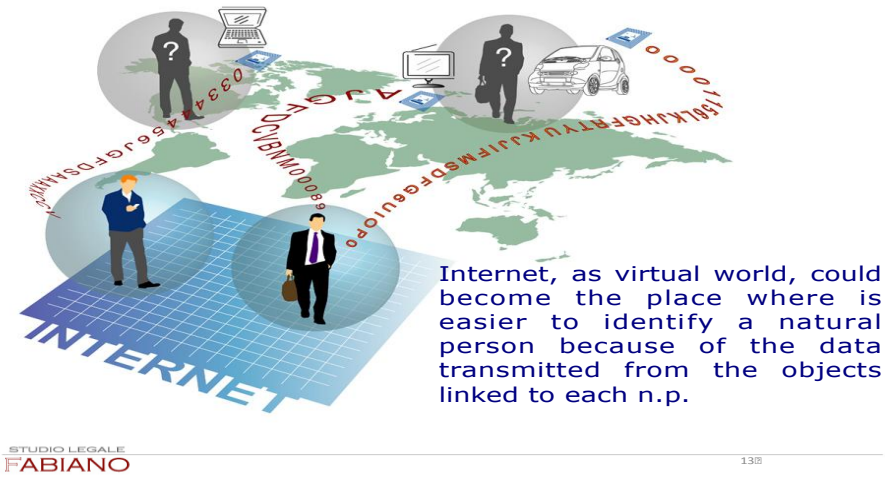


Figure 2 - The risks of being part of a virtual world

As presented in details in the Ethics Factsheet summarizing the findings of the ethics subgroup of the IoT Expert Group of DG Connect[11] the main identified issues regarding Ethics in IoT are:

- **The risk of social divides**: although many societal benefits are envisioned for IoT, their deployment and spreading may not be uniform across the population, creating a risk of an increased digital divide (between those who can afford and use the new applications and services and those who cannot). This risk is reinforced may even amplify in a "knowledge divide", between those who know and understand the technologies behind an IoT world and those who don't and who are therefore unable both to take full profit of it and to avoid potential dangers.
- The key issue **of trust and reliance on IoT** which is mostly linked, but clearly not limited to the respect of privacy and data security. The massive deployment of IoT enabled technologies and services will pose the question of their reliability and how, when, and why the user can, or has to rely on these new services in a trustful relationship. This need for a trustful relationship and the risk associated are even stronger in the case of "smart", context aware applications who advise decisions to the end user. This pleads for the need for openness and reputation / ranking systems as strong needs to establish this trust.
- The risk of a **blurring of context** in the society perception of what is private and public, what is virtual and what is real. This evolution of society values and perception is not necessarily an issue in itself, but it has to be understood, monitored and reflected upon to make sure that it doesn't result in additional issues or increase existing risks (such as the risk of social divides, especially between different age groups).
- The **non neutrality of the IoT metaphors and vocabulary**. Many terms and metaphors (such as the "smart"-things) used to describe IoT technologies, product and services assume that IoT will ease the lives of people, and they convey this meaning and raises expectations. This non neutrality and the associated expectations are important to be understood not only by the stakeholders defining the IoT but also by the targeted market.
- The necessity of **a social contract between object and peoples**. This necessity arises from the stronger and stronger reliance of societies on technologies envisioned in the IoT vision. As IoT objects are more and more autonomous, connected and involved in our lives, this may result in loss of control for users (as object take decisions for them) and in blurring of responsibilities for stakeholders (whose in the end really responsible for the decision). This pleads for a strong reflection on how IoT objects should behave and interact with people and

[11] http://ec.europa.eu/digital-agenda/en/news/conclusions-internet-things-public-consultation

with each others. A need that is furthermore reinforced in the case of context awareness by the ability of objects to create profiles of users and stakeholders based on the data gathered.

- And the **issue of informed consent and obfuscation of functionalities** which here again rejoin the privacy and data protection issue (without being limited to it). The actual understanding of what is happening in IoT scenarios, which is necessary for a truly "informed" consent by the user, is complicated by the strong tendency of IoT deployments to be actually nearly invisible as communicating objects are miniaturized, hidden, and their true features obfuscated. This pleads for an ability to make IoT deployment visible for inspection, education and explanation needs.

4.1.3. Privacy, Data protection and the IoT

As described above, in addition to these "high-level" Ethics interrogations related to IoT, the main, more immediate and practical questions relate to the risk of privacy breaches and the necessity to ensure the security of the huge quantities of data gathered and used by IoT systems. As described above (section 4.1.1), these privacy and security issues are essential because of their major impact on the development and acceptance of IoT.

Based on the findings of the privacy and security subgroup of the IoT Expert Group of DG Connect[12], and their analysis in the BUTLER project[13], the main identified privacy and data protection issues in IoT are:

- **Continuity and availability of services:** As the deployment of IoT spreads and more and more systems and persons rely on these new products, applications and services, the issue of continuity and availability of the services rises. The strong integration of IoT devices in our day to day lives, and especially in critical services (such as health, security, and energy) increase the impact of a potential loss of service.
- **Sensibility of user data and contextualization of risks:** As Smart services gather more and more information on the user (willingly or even without notice), the question of the sensibility of these data, arise. The internet of things complicates this issue as it gathers more and more information that, despite a harmless appearance, can turn out to become sensitive when analyzed on a large scale. For example the collection of household power consumption can seem to hold no important privacy issues, however these data when statistically analyzed can reveal much on the content of the user home and his day to day habits. The actual sensibility of gathered information is therefore not always known at the time when data gathering is decided and / or accepted by the user. In an IoT world, the risks related to privacy and data security are dependant of the context and purpose in which data is gathered, and used. And this context can be evolving, which support the need for a context-aware management of security and data protection.
- **Security of user data**: The user data must therefore be protected against unauthorized access, and this security should be ensured at each level of communication. The multiplication of communicating devices characteristic of the Internet of Things therefore increases the difficulty of this protection as the number of link to be protected increases. The potential impact of security breaches is also on the rise as the data stored have more and more applications, and thus give more and more information on the user and give more and more access to critical parts of our lives. (Increasing risks linked to identity theft and electronic identification).

[12] http://ec.europa.eu/digital-agenda/en/news/conclusions-internet-things-public-consultation

[13] Deliverable 2.1 requirements, specifications and security technologies for iot context-aware networks and 3.1 architectures of butler platforms and initial proofs of concept available here: http://www.iot-butler.eu/download/deliverables

- **Management of data:** Even when the security of the user data can be guaranteed against unauthorized access, the question of the actual management and storage of the information by the service provider remains. Questions such as: “How much data is collected to provide the service?”, “Is this strictly necessary?”, “Who is responsible to handle these data?”, “Who has access, how and when to the data?”; can be expected from the user.
- **Ownership, repurposing and communication of data:** The question of the ownership of the data collected is also central to the IoT Ethics issue: getting propriety or access to user data and reselling these data can be a significant source of revenue. The monetization of user data can raise several issues: how is the additional revenue shared between the service provider and the user? How aware is the user of this use of his data? How much control does he have on it? What are the third parties who get access to the data and for what?
- **Captivity of data:** Even as the service is becoming more and more used and accepted by the user, the ethics question remains: what happens to the user data if the user leaves the service? And how feasible is it for a user or consumer to change service provider once he has been engaged with one for a significant time? These questions are important to avoid consumer captivity through data that would result in an unfair advantage, destroying competition with all the eventual consequences (suppression of consumer choice, degradation of user service and reduction of innovation).
- **Applicable legislation and enforcement:** Given the global nature of IoT and the number of stakeholders necessarily involved in an IoT deployment, the question of responsibility and applicable legislation arise. This is reinforced by the fact that in a truly “Internet” of things vision the different actors will be spread across different countries and regions, increasing the number of potential legislation involved. This issue impact not only the users, which may be confused on which legislation the service he uses follows, but also the policy makers and the whole IoT value chain as developing IoT applications and deployment without a clearly identified chain of responsibilities and applicable law represent a strong business risks.
- **Availability of information:** Finally in a world where technical and legal complexity increase, the quality of the information available to the user is key to the management of the ethical issues: the service provider must ensure not only that the information is available, but that it is presented in a way that ensure it is correctly understood by the user.

All these concerns leads to the so called “Privacy Paradox” : By collecting personal data, better “personalized’ services can be offered to the users; but on the other side, these personal data can be collated, linked with transactional data, processed by powerful data mining techniques and assembled into user profiles that may become so detailed, that identification becomes possible. Once this “personal data” has been disclosed, the owner of the data cannot control how the collector will use the data. With this conception, should the user thus refrain from disclosing personal data? And therefore refuse life improving services?

4.2. Initial Ethical requirements in BUTLER

In deliverable D1.1 the BUTLER project team not only described vertical scenarios with exemplified use cases, we also identified a number of global non functional requirement and global constraints that address topics common to all vertical domains and cover the full horizontal view of BUTLER.

Of these global constraints and requirements quite a few are related to ethical topics which are mostly interrogation of higher level than the requirements defined in BUTLER, and more therefore focus on the more practical issues of privacy and data protection. It was therefore decided to highlight these constraints and requirements in this document, to give a more concise view on the ethical topics already covered within the BUTLER project.

In Annex A: Global Requirements and Constraints from D1.1 you can find four tables that show these requirements and constraints, keeping the original requirement ID, description and related use case IDs from D1.1, but occasionally giving a more in depth explanation in the rationale, if that seemed necessary to highlight the link to the context of this document.

Also the requirements have been split into requirements and constraints that

- specifically address ethical – and especially privacy – issues and try to solve them,
- and into requirements or constraints that may raise additional privacy or other ethical issues and need to have ethical considerations designed into their solution from the very beginning.

4.3. End user perception of privacy, ethics and IoT

4.3.1. End user interviews

To measure the public perception of potential IoT use cases in the general public, the BUTLER project organized interviews with potential end users. More than 60 interviews were organized in 6 European countries (Switzerland, France, Italy, Spain, Germany, and Luxemburg). The interviews lasted around 1 hour each, and were open discussions with limited direction from the interviewer (to limit as much as possible direct influence and maximize interviewer objectiveness). The interviews consisted in a brief presentation, through a “comic-book” image and brief description of some (10 to 15) of the use cases selected by the BUTLER project as most relevant[14]. The interviewees were selected to represent diverse profiles (based on the personas identified in the use case selection of the BUTLER project), all with no specific knowledge or experience in ICT technologies. Annex B presents the methodology, material and initial results of the BUTLER end user interviews.

These interviews were not directly focused on ethics, privacy and data protection issues as the interviewees were asked to provide us their general feeling and interrogations about the use case presented. However as the interviewer asked both for positive and negative feedback, they directly mentioned “ethics and privacy”. In the examples, the interviews reflect to an extant what potential customers have to say about these issues.

Regarding ethics concerns:

- The most frequent comment concerned the risks of social divide and loss of autonomy in an IoT society. As stated above almost 50% of interviewees where concerned about the possibility that IoT applications might lead to greater isolation and loss of contact with other human beings.

Regarding privacy:

- For most privacy is not a problem, as they are not directly aware of it
- On the other hand, some are very critical and hence not prepared to use BUTLER like systems

[14] The use cases and associated personas selected by the BUTLER project are presented in Deliverable 1.1 – Requirements and Exploitation Strategy http://www.iot-BUTLER.eu/wp-content/uploads/downloads/2012/07/Deliverable-1-1-Requirements-and-exploitation-strategy-submitted120214.pdf

There seems to be a wide selection of attitudes towards data privacy, ranging over

- My data is open to anybody, I have nothing to hide
- I know, I should care more about privacy issues, but functionality and being part of things is so much more important to me
- I'm somewhat worried, so I only do business with companies I can trust and hope they will take care of my data
- My data is mine, I decide who gets access and why
- My data is private, nobody gets access to it

What can also be seen is that the closer an application or a service gets to the personal life of a customer and the more personal and therefore sensitive the data is perceived to be, the more customers are worried about data privacy.

Customers in general were much more reluctant about sharing their health data or data about their personal energy usage, than they were about sharing shopping habits or travelling information. The identification of ethical and privacy issues in the general public also strongly depends from the technology used to gather the data. For example interviewees were usually much more sensitive to use case involving cameras than other sensors, even if the potential breaches to their privacy were stronger without camera. This can be explained by the negative image of camera surveillance ("big brother") and a lack of understanding of what data can actually be gathered by other sensors and what information can be obtained based on these data.

These results lead us to conclude that:

- Ethics and privacy issues can have a strong impact on the development and deployment of IoT, as the end-users that actually identify potential threats to their privacy or way of life are very strongly critical of the use case presented.
- The views and analysis of independent experts are strongly needed if we want to fully address ethics and privacy concerns beforehand as most end-users are not able to directly identify the potential impact of such disruptive technologies.
- A stronger effort could be put to raise people awareness and understanding of technology.

4.3.2. European Commission's public consultation on the Internet of Things

These end users feedback gathered within the BUTLER are complemented by the conclusions of the Internet of Things public consultation organized by the European Commission[15].

> "The public consultation was held between April and July 2012600 people, associations and various groups from academics and civil society, as well industry players responded to the consultation. Through the public consultation, the Commission sought views on an a policy approach to foster a dynamic development of Internet of Things in the digital single market while ensuring appropriate protection and trust of EU citizens."

This study showed a strong concern on ethics and privacy issues.

[15] http://ec.europa.eu/digital-agenda/en/news/conclusions-internet-things-public-consultation

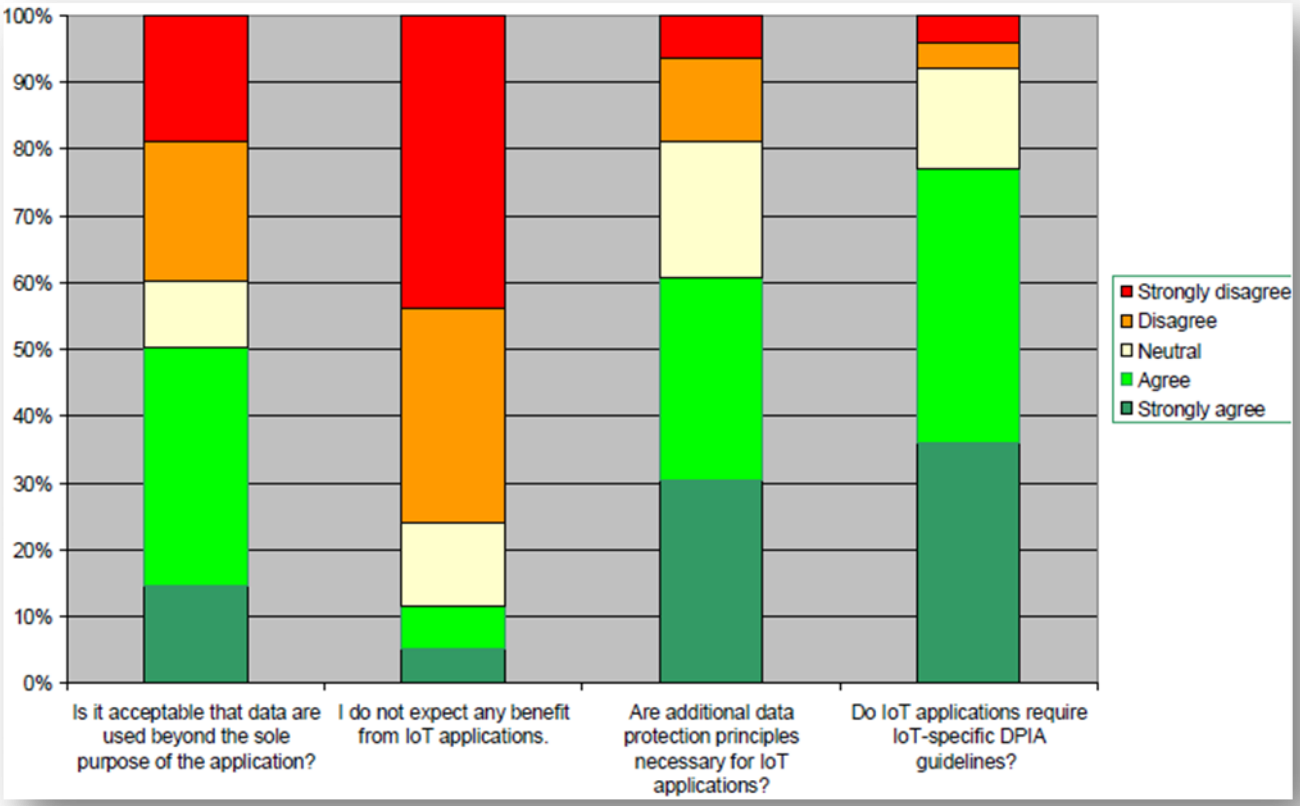


Figure 3 - Privacy concerns in the public consultation on the IoT

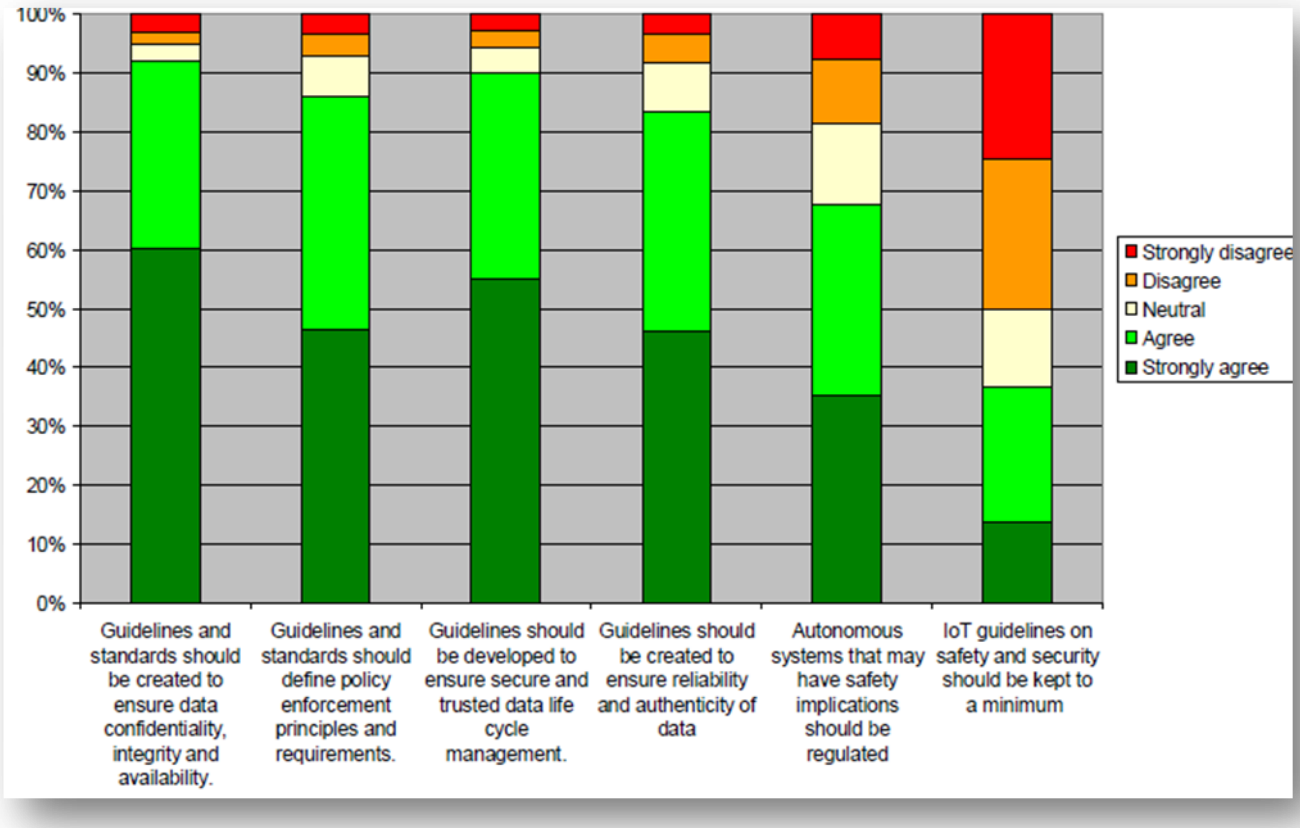


Figure 4 - Safety and security concerns in the public consultation on the IoT

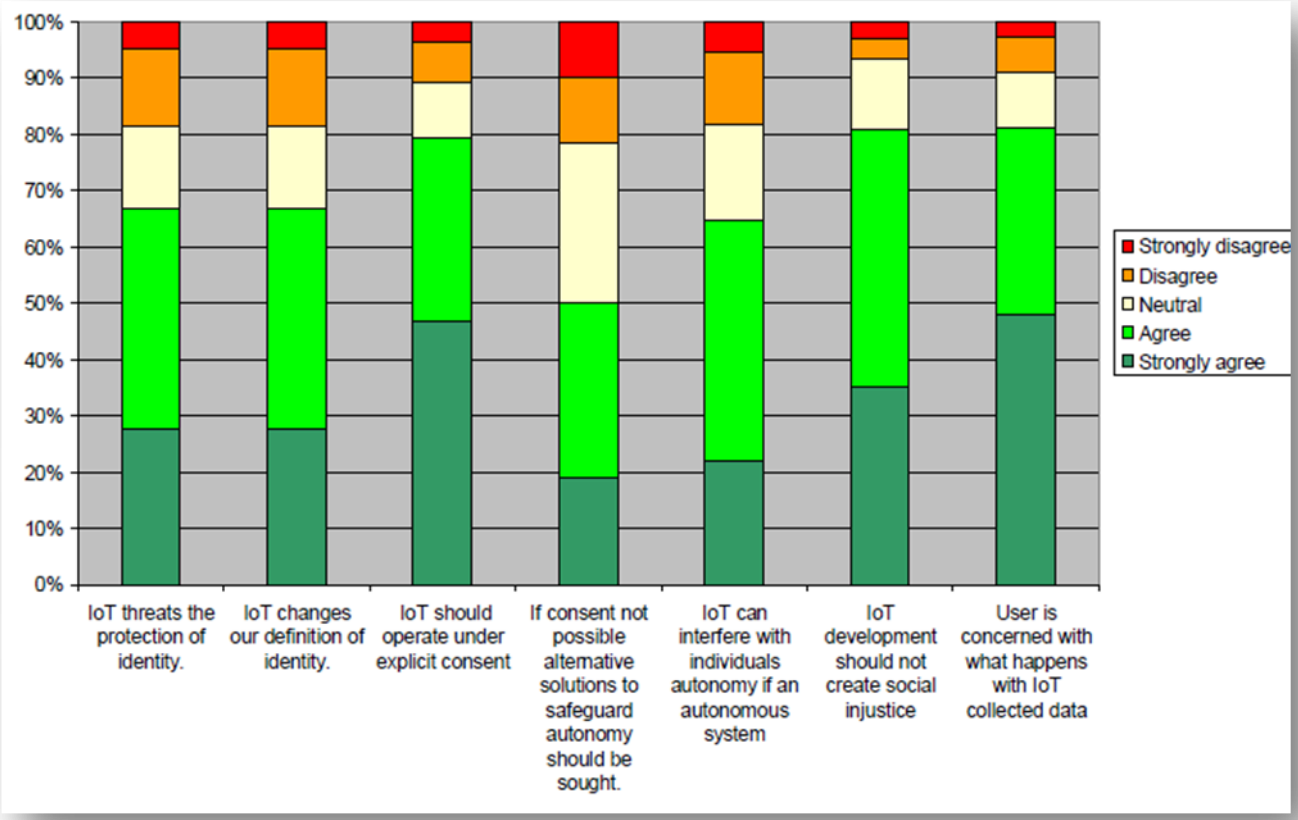


Figure 5 - Ethics concerns in the public consultation on the IoT

These result obtained from people already knowledgeable on IoT further reinforce the conclusions of the BUTLER interviews on the importance of ethics and privacy issues and the need for both independent experts views and increased public awareness and understanding.

4.4. Further analysis of Ethics and Privacy requirements

4.4.1. Challenging with External Experts

To get a more complete understanding of potential Ethics and Privacy Experts, a specific thematic group has been created with BUTLER external member group[16].

The following chapter presents an overview about the topics and key questions, which have been discussed during the BUTLER project sessions dedicated to the privacy & ethical issues. The main goal of the workshops was: opinions exchange, identifying as many issues as possible from different point of view, challenging and sharing the insights with the partners and experts[17].

For this purpose a set of use cases resulting from D1.1 has been analysed. The selected use cases have been broken down to the aspects relevant to ethical and privacy issues so that a set of interesting topics can be identified. The following section illustrates a summary of the presentation[18], which have been a base for the discussions.

Looking at the main goals of BUTLER, we identify 2 significant aspects worth to be considered in terms of ethical & privacy issues[19]:

1. **Location and Context Awareness –** This is far more than the simple location information.

   Location and context awareness as understood by BUTLER includes:

   - **Semantic Location** (in/out; grouped/individual; girth and spread of user groups; border/centre, proximity, direction, etc)
   - **Duration, Motion, Repetition** and other **Geo-Temporal** information.

2. A System that adapts to Evolving User Needs through **Behaviour Modelling** and **Data Mining.**

   Collecting data from user (proactive) input only is too slow and not accurate enough for an self- learning system. One of the objectives within BUTLER therefore is **to digitize human behaviour** and to **recognize intent through external observation** of human behaviour, human decisions and their course of actions.

To trigger the discussions for each of these aspects 2 use cases have been selected from the "One day in 2020" and analyzed.

1. **Location**& **Context Awareness**
   - 1A) Use Case: Searching for a parking slot
   - 1B) Use Case: Getting visit
2. A System that adapts to evolving User Needs through **Behaviour Modelling** and **Data Mining**
   - 2A) Use Case: Doctor's visit arrangement
   - 2B) Use Case: Washing at the "right" time

In following section the discussed use cases will be described in detailed way.

[16] External discussion partners: Trevor Peirce, Job Timmermans, Nicola Fabiano, Rob von Kranenburg , Gabriela

[17] The discussions have been initiated in the Ethical Session in the IoT Week in Venice and beencontinued in Luxembourg with representatives of legal, technical and commercial and sociological background.

[18] Source: Swisscom, Katharina Liebrand

[19] Source: DOW BUTLER

4.4.1.1. Searching for a parking slot

"Donald is late for work and needs a parking slot close to his office as soon as possible."

Figure 6 - Smart City UC: Searching for a parking slot.

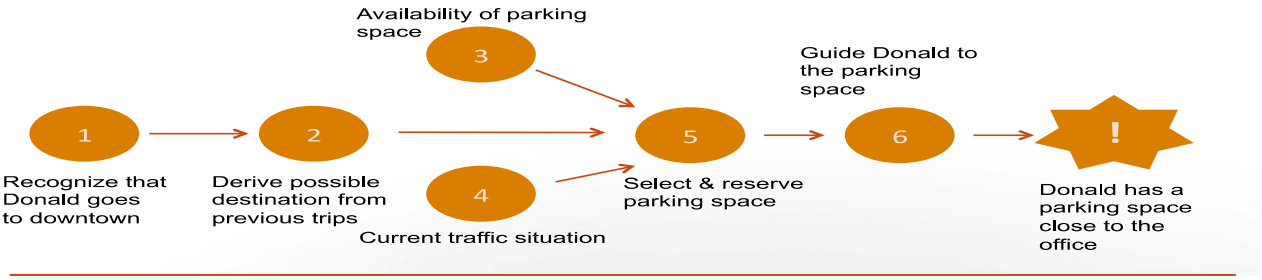


Figure 7–Bottom-Up Analysis: Information Flow Process

Looking at the illustrated process several issues concerning with data privacy can be already identified:

- The BUTLER service collects a lot of data very specific to Donald
- The car insurance may validate contract data about driving behaviour
- The city may use such data for toll collection purposes
- Other parties obtaining such data may also use this for purposes like advertising.

This example in the SmartCity area includes the gathering of data to:

monitor traffic conditions in a specific area

predict possible problems and alert drivers in the area to them

thus ensuring that drivers find parking spaces quickly and get off the road

This might show only one of many cases addressing a series of questions about: Responsibility, Accountability and Liability. To be more specific, following questions might come up in this context:

- **Who** will manage my personal data? **Who** is entitled at all to manage it?
- **How** will be my personal data managed?
- **Where** will my personal data be and how much influence do I have on managing the data?
- **Who** has the final ownership?

Going back to the use case: Donald as a frequent driver may very well have consented to this use of his location data and movement profile. Because these kind of services are expensive and somebody needs to pay for them he granted his car insurance company access to this data in exchange for providing him with this service[20].

[20] Such scenario already exist to some extent as described here: http://telematicsnews.info/2013/02/11/40966_f4113/

Now let imagine the following situation: Donald car insurance decides to charge different premiums depending on the kind of traffic he normally encounter on his way to work or how many kilometres he drives in a normal week or even how fast he drives. Regarding this, additional questions might come up:

- Should this be covered by the consent he gave for them to use his data?
- Was it really in his capacity to foresee this kind of consequences when he gave his consent?
- And what if all insurances ask for that kind of data access and otherwise they will not even give him insurance at all? Would he really agree that his consent is given voluntarily in such a scenario?
- And what if the local government proposed to use that kind of information for taxation purposes, road pricing or the like.

4.4.1.2. Getting visit

"Donald sees that his friend has arrived at holiday home and remote face and voice identification system prompts Donald to grant him access."

Figure 8: Getting visit I.

Figure 9 -Getting Visit II

Looking at the simplified process of data transformation, we see already that there is a lot of information needed to make the "Door is opened, visitor can enter" successful. Additionally following implications have been identified:

- The BUTLER service collects a lot of data very specific to Donald's visitors as well as himself
- Donald may decide to sell „his" data collection to interested parties, but **who owns** the **visitor's data**

or here: http://www.reuters.com/article/2013/02/06/telefonica-car-idUSL5N0B69P220130206

- Donald's visitors might prefer to visit incognito, but the BUTLER service **identifies** them **anyway**
- Thieves might access the data to build inhabitant profiles and decide when the best time for breaking in is.

On the other side ….Imagine Donald is a real fan of smart objects:

- So nearly everything Donald possesses includes some kind of chip, sender, RFID and the whole environment is full of sensors and readers…
- On the whole he does not mind that all sorts of institutions, organisations or people have access to the data collected by these objects, so he is really generous with giving access
- Or perhaps he considers himself to be a producer of data and is selling access to his data, after all, the data is anonymised, access to it is secure and follows the minimal disclosure principle

Regarding the situations described above, following questions may appear:

- How anonymous is the data then?

Donald lives in a small village of 1000 inhabitants. How difficult can it be to find out who he is, if you know when he likes to go shopping, what he likes to buy, where he normally does his grocery shopping as opposed to shopping for clothes, that he really like books, what his living situation is, what type of car he drives etc.

- What about informed consent?
  - What if he sells to some fashion company what he does know about his "friends" or neighbours, simply by having a clothes reading sensor in his house, which will read the information from their clothes.
  - Is the fashion company then allowed to use that information?
  - Or will there be legislation forcing me to disclose in detail the presence of sensors in my home to all my visitors, so they can properly consent to visiting me?
  - Wouldn't thieves just love that information, to better prepare how to rob my house, when I'm not in?

4.4.1.3. Doctor visit arrangement

"Madeleine's blood pressure is too high so a video conference with her doctor is arranged for later during the day"

Figure 10: Doctor visit arrangement I.

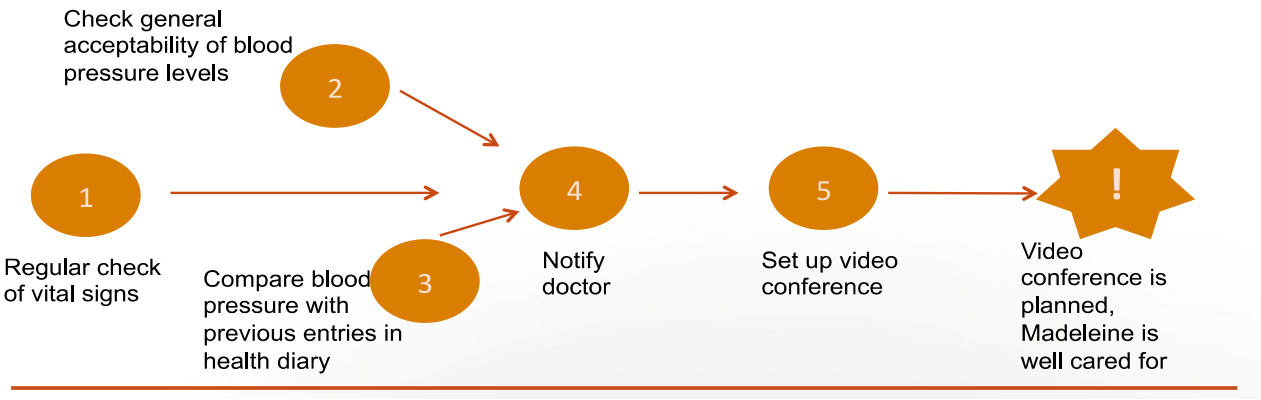


Figure 11: Doctor visit arrangement II.

Regarding the data transformation process closely it might be concluded that:

- The BUTLER service collects a lot of data very specific to Madeleine's health status, her environment and her activities
- Madeleine might have other plans and not want to talk to a doctor, her high blood pressure might have non health reasons
- Madeleine might feel constantly controlled and supervised and loses her personal freedom

The insurance agency might charge more according to the BUTLERs activities (patient classification).

- How much influence has Madeleine here on BUTLER reaction?

As an elderly person, Madeleine is able to continue to live independently because the BUTLER is taking care of some of the mundane tasks and keeping a continuous watch over her, e.g.

- realise that she didn't turn off her iron or the stove and do this for her
- keep track of the medication I should take or which she should better not take and remind her accordingly
- notify a care-giver or an ambulance, if she has not moved for a certain amount of time or has not gotten up at the usual time of day

Obviously she will have consented to this use of her behaviour profile and sensor data and will have agreed on whom should be notified in a case of emergency…

But let's suppose she has recently been diagnosed with a terminal kind of cancer and decide to do all the things she has always wished to do: How independent is her independent living anyway, if constant monitoring and observation is the rule and my every action and intent is predicted by the system?

4.4.1.4. Washing at the "right" time

"Daisy's washing machine and the dishwasher take advantage of the cheap electricity and start their work"

Figure 12: Washing at the right time.

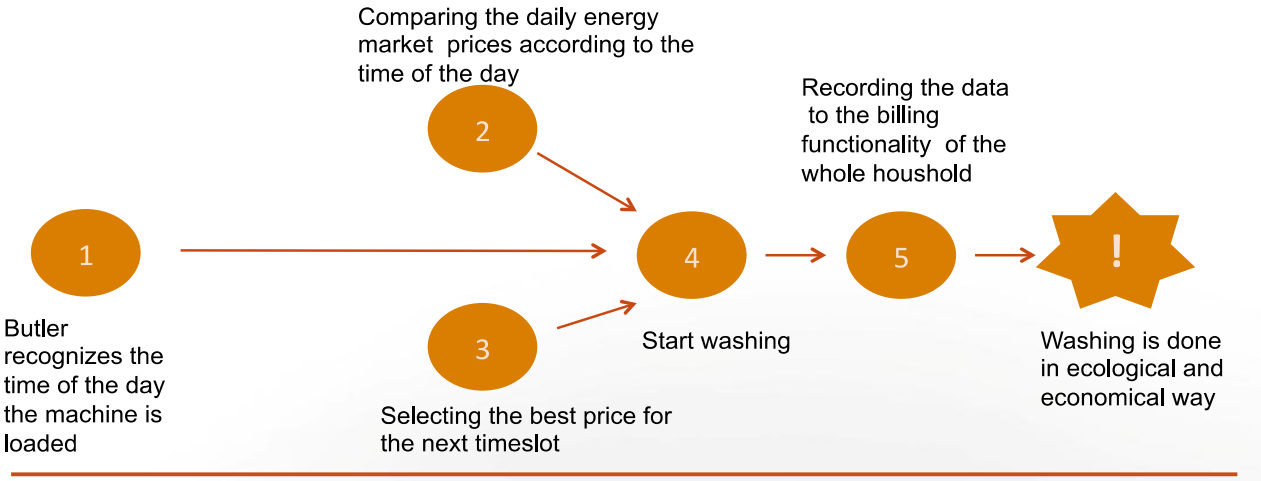


Figure 13: Washing at the right time – Data Transformation Process

Looking at this transformation process closely following concerns may arise:

- The BUTLER service collects a lot of data very specific to the behavioural patterns, timing, frequencies Daisy`s household
- The energy partner may use such data for purposes like advertising to the utility company for instance
- Other parties obtaining such data may also use this for purposes like advertising

So how much control will be given to the user at the end?

At first glance the story has a lot to offer for a society which desperately needs to save energy, be more environmental aware and at the same time does not want to give up the accustomed standard of living

So far why not use machines to manage a system which makes sure, that everybody uses their fair share of resources at a time while still allowing everybody to continue living in style?

Our electric appliances will know when to start and when to stop, according to the price and availability of - preferably green – energy, our plants – both at home and perhaps on a larger scale even in our fields and greenhouses - will be watered and fed according to their needs and with the common good of water preservation and ecological responsibility in mind

But...

- Who is taking advantage of the solution? Why should the consumer have to pay for sensors and meters which so far mostly seem to deliver a benefit to the energy providers?
- Do smart meters really need to measure energy consumption to a very accurate degree and every second or so?
- What information exactly can be derived from that data, who owns the data and what will happen with this information?

4.4.1.5. Conclusions of use case analysis

Concluding all the discussions led in the BUTLER context, there are 3 main statements to be highlighted:

- While (mis-)usage of data seems to be a common pattern, **the (unintent) use** of it may happen in many different ways. Thus the possibilities what can be done with such **data needs to be evaluated** with every new service.

- **Technical Standards** which services can be in compliance with, may help to **protect users privacy** whithout impacting the experience in using the service.

- **Raising the awareness** for such topics may help to guide **customers** to choose offers that comply to such standard and achieve a higher level of data privacy in a world of IoT

Figure 14: Ethical Issue Session BUTLER – Conclusions from the Ethical Issues discussions

4.4.2. Legal Overview and Current Situation on Privacy

To further complement our understanding of Privacy and Data Security issues, one of the industrial partners of the project (Swisscom) has led a detailed legal overview of the current situation:

4.4.2.1. Current Situation

4.4.2.1.1. Historical Context

The right to privacy is a highly developed area of law in Europe. All member states of the European Union (EU) as well as of the European Free Trade Association (EFTA) are signatories of the European Convention on Human Rights (ECHR; effective on 3 September 1953). Article 8 of the ECHR provides a right to respect for one's "private and family life, his home and his correspondence," which has been given by the European Court of Human Rights (ECtHR) a very broad interpretation in its jurisprudence.

In 1980, in an effort to create a comprehensive data protection system throughout Europe, the Organization for Economic Cooperation and Development (OECD) issued its “Recommendations of the Council Concerning Guidelines Governing the Protection of Privacy and Trans-Border Flows of Personal Data.” The seven principles governing the OECD’s recommendations for protection of personal data were:

1) Notice—data subjects should be given notice when their data is being collected;
2) Purpose—data should only be used for the purpose stated and not for any other purposes;
3) Consent—data should not be disclosed without the data subject’s consent;
4) Security—collected data should be kept secure from any potential abuses;
5) Disclosure—data subjects should be informed as to who is collecting their data;
6) Access—data subjects should be allowed to access their data and make corrections to any inaccurate data; and
7) Accountability—data subjects should have a method available to them to hold data collectors accountable for following the above principles.

The OECD Guidelines, however, were nonbinding, and data privacy laws still varied widely across Europe. The US, meanwhile, while endorsing the OECD's recommendations, did nothing to implement them within the United States.

In 1981, the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data was negotiated within the Council of Europe (Effective on 1 October 1985). This convention obliges the signatories to enact legislation concerning the automatic processing of personal data, which many duly did.

The European Commission realised that diverging data protection legislation amongst EU member states impeded the free flow of data within the EU and accordingly proposed the Data Protection Directive.

The Data Protection Directive of 24 October 1995 (officially Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data; hereinafter "Data Protection Directive") is a European Union directive which regulates the processing of personal data within the European Union. It is an important component of EU privacy and human rights law.

The directive regulates the processing of personal data regardless of whether such processing is automated or not. Furthermore, it incorporates all seven principles of the OECD recommendation.

4.4.2.1.2. Scope of the Data Protection Directive

Personal data are defined as "any information relating to an identified or identifiable natural person" ("data subject"). By consequence, an identifiable person is someone who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity (art. 2 a Data Protection Directive).

This definition is meant to be very broad. Data are "personal data" when someone is able to link the information to a person, even if the person holding the data cannot make this link. Some examples of "personal data" are: address, credit card number, bank statements, criminal record, etc.

The notion processing means "any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction;" (art. 2 b Data Protection Directive).

The surveillance of the compliance of the Data Protection rests on the shoulders of the "controller", meaning the natural or legal person, public authority, agency or any other body which alone or jointly with others, determines the purposes and means of the processing of personal data (art. 2 d).

The data protection rules are applicable not only when the controller is established within the EU, but whenever the controller uses equipment situated within the EU in order to process data (art. 4). Controllers from outside the EU, processing data in the EU, will have to follow data protection regulation. In principle, any online business trading with EU citizens would process some personal data and would be using equipment in the EU to process the data (i.e. the customer's computer). As a consequence, the website operator would have to comply with the European data protection rules.

The proposed new European Union Data Protection Regulation extends the scope of the EU data protection law to all foreign companies processing data of European Union residents.

4.4.2.1.3. Supervisory authority and the public register of processing operations

Each member state must set up a supervisory authority. It has to be an independent body that will monitor the data protection level in that member state, give advice to the government about administrative measures and regulations, and start legal proceedings when data protection

regulation has been violated (art. 28 Data Protection Directive) Individuals may lodge complaints about violations to the supervisory authority.

4.4.2.1.4. Transfer of personal data to third countries

"Third countries" is the term used in EU legislation to designate countries outside the European Union. Personal data may only be transferred to third countries if that country provides an adequate level of protection. Some exceptions to this rule are provided, for instance when the controller himself can guarantee that the recipient will comply with the data protection rules.

The Directive's Article 29 created the "Working party on the Protection of Individuals with regard to the Processing of Personal Data," commonly known as the "Article 29 Working Party". The Working Party gives advice about the level of protection in the European Union and third countries.

The Working Party negotiated with U.S. representatives about the protection of personal data, the Safe Harbour Principles were the result. According to critics, the Safe Harbour Principles do not provide for an adequate level of protection, because they contain fewer obligations for the controller and allow the contractual waiver of certain rights.

4.4.2.1.5. Implementation by the member states

As EU directive, the Data Protection Directive is addressed to the member states but is not legally binding for citizens in principle. The member states must transpose the directive into internal law. The Data Protection Directive had to be transposed by the end of 1998. Meanwhile, all member states have enacted their own data protection legislation. On the other hand, with the enlargement of the EU, there are 27 different Data Protection legislations within the EU.

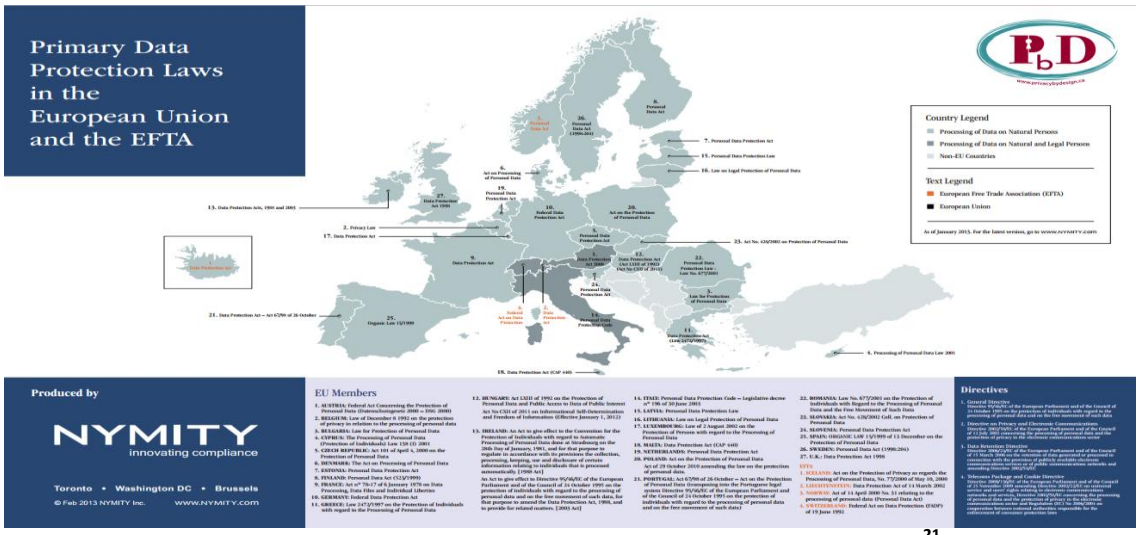


Figure 15 - Data Protection Laws in the European Union and EFTA[21]

4.4.2.1.6. Directive on Privacy and Electronic Communications

Overview

The Directive 2002/58 on Privacy and Electronic Communications, otherwise known as E-Privacy Directive, was adopted in 2002 as a complement to the existing Framework of the Data Protection Directive. It deals with the regulation of a number of important issues such as confidentiality of information, treatment of traffic data, spam and cookies. All EU countries were supposed to incorporate the Directive into their national law by October 31, 2003. This Directive has been

[21]Map of the data protection laws in Europe :http://www.privacybydesign.ca/content/uploads/2012/11/PrivMap-EU_Data_Protection_pbd.pdf source: www.privacybydesign.ca

amended twice since its inaction (Directive 2006/24/EC, OJ L 105, 13.4.2006; Directive 2009/136/EC OJ L 337).

The 2009 amendment replaced the opt-out rule with an opt-in consent rule. The majority of the Member States requires explicit, affirmative consent for each website. A minority part defends the point of view that existing browser settings would remain adequate, since they conveyed "implicit consent."

Scope

The E-Privacy Directive has been drafted specifically to address the requirements of new digital technologies and ease the advance of electronic communications services. The Directive complements the Data Protection Directive and applies to all matters which are not specifically covered by that Directive. In particular, the subject of the Directive is the “right to privacy in the electronic communication sector” and free movement of data, communication equipment and services.

The Directive does not apply to Titles V and VI (Second and Third Pillars). Likewise, it does not apply to issues concerning public security and defence, state security and criminal law. At present, the interception of data is covered by the new EU Data Retention Directive the purpose of which is to amend the E-Privacy Directive.

Contrary to Data Protection Directive, which specifically addresses only individuals, Article 1(2) makes it clear that E-Privacy Directive also applies to legal persons.

The article is technology neutral, not naming any specific technological means which may be used to store data, but applies to any information that a website causes to store in a user's browser. This reflects the EU legislator’s desire to leave the regime of the directive open to future technological developments.

The addressees of the obligation are Member States, who must ensure that the use of electronic communications networks to store information in a visitor's browser is only allowed if the user is provided with “clear and comprehensive information”, in accordance with Data Protection Directive, about the purposes of the storage of, or access to, that information; and has given his or her consent.

Main provisions

The first general obligation in the Directive is to provide security of services. The addressees are providers of electronic communications services. This obligation also includes the duty to inform the subscribers whenever there is a particular risk, such as a virus or other malware attack.

The second general obligation is for the confidentiality of information to be maintained. The addressees are Member States which should prohibit listening, tapping, storage or other kinds of interception or surveillance of communication and “related traffic”, unless the users have given their consent or conditions of Article 15(1) have been fulfilled.

Data retention and other issues

The directive obliges the providers of services to erase or anonymise the traffic data processed when no longer needed, unless the conditions from Article 15 have been fulfilled. Retention is allowed for billing purposes but only as long as the statute of limitations allows the payment to be lawfully pursued. Data may be retained upon a user’s consent for marketing and value-added services. For both previous uses, the data subject must be informed why and for how long the data is being processed.

Subscribers have the right to non-itemised billing. Likewise, the users must be able to opt out of calling-line identification.

Where data relating to location of users or other traffic can be processed, Article 9 provides that this will only be permitted if such data is anonymised, where users have given consent, or for provision of value-added services. Like in the previous case, users must be informed beforehand of the character of information collected and have the option to opt out.

Unsolicited e-mail and other messages

Article 13 prohibits the use of email addresses for marketing purposes. The Directive establishes the opt-in regime, where unsolicited emails may be sent only with prior agreement of the recipient. A natural or legal person who initially collects address data in the context of the sale of a product or service, has the right to use it for commercial purposes provided the customers have a prior opportunity to reject such communication, either where it was initially collected or subsequently. Member States have the obligation to ensure that unsolicited communication will be prohibited, except in circumstances given in Article 13.

Two categories of emails (or communication in general) will also be excluded from the scope of the prohibition. The first is the exception for existing customer relationships and the second for marketing of similar products and services [11] The sending of unsolicited text messages, either in the form of SMS messages, push mail messages or any similar format designed for consumer portable devices (mobile phones, PDAs) also falls under the prohibition of Article 13.

Cookies

The Directive provision applicable to cookies is Article 5(3). Recital 25 of the Preamble recognizes the importance and usefulness of cookies for the functioning of modern Internet and directly relates Article 5(3) to them but Recital 24 also warns of the danger that such instruments may present to privacy. The change in the law does not affect all types of cookies. For cookies that are deemed to be 'strictly necessary for the delivery of a service requested by the user' the consent of the user is not needed. An example of a 'strictly necessary' cookie is when you press 'add to basket' or 'continue to checkout' when shopping online. It is important that the browser remembers information from a previous web page in order to complete a successful transaction.

The regime set-up can be described as opt-in, effectively meaning that the consumer must give his or her consent before cookies or any other form of data is stored in their browser. The UK Regulations allow for consent to be signified by future browser settings, which have yet to be introduced but which must be capable of presenting enough information so that a user can give their informed consent and indicating to a target website that consent has been obtained. Initial consent can be carried over into repeated content requests to a website. The Directive does not give any guidelines as to what may constitute an opt-out, but requires that cookies, other than those "strictly necessary for the delivery of a service requested by the user" are not to be placed without user consent.

4.4.2.1.7. Data Retention Directive

On 15 March 2006 the European Union adopted the Data Retention Directive (Directive 2006/24/EC), on "the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC". The Directive requires Member States to ensure that communications providers retain, for a period of 6 months and 2 years, necessary data as specified in the Directive.

The data is required to be available to "competent" national authorities in specific cases, "for the purpose of the investigation, detection and prosecution of serious crime, as defined by each Member State in its national law".

The Directive covers fixed telephony, mobile telephony, Internet access, Internet email and Internet telephony. Member States were required to transpose it into national law within 18 months - i.e. no later than September 2007. However, they may if they wish to postpone the application of the Directive to Internet access, Internet email and Internet telephony for a further 18 months after this

date. A majority of Member States exercised this option. By now, all Member States have transposed the Directive into their national law.

A report evaluating the Directive was published by the European Commission in April 2011. It concluded that data retention was a valuable tool for ensuring criminal justice and public protection, but that it had achieved only limited harmonisation. There were serious concerns from service providers about the compliance costs and from civil society organisations which claim that mandatory data retention was an unacceptable infringement of the fundamental right to privacy and the protection of personal data. The Commission is now reviewing the legislation.

4.4.2.2. Future legislation

4.4.2.2.1. Reform

The European Commission plans to unify data protection within the European Union with one single law, the General Data Protection Regulation (GDPR). Compared to a Directive, a Regulation does not need to be transposed into internal law of each EU Member. The present Directive will be completely replaced by the Regulation.

The reform of the current EU Data Protection Directive became necessary as it does not consider sufficiently important aspects like globalization and technological developments like social networks and cloud computing.

Therefore, new guidelines for data protection and privacy were required and a proposal for the regulation has been released on 25 January 2012. The adoption is aimed for 2014 and the regulation is planned to take effect in 2016 after a transition period of 2 years. Discussions regarding the specific contents are still ongoing.

The European Data Protection Regulation will replace the current Data Protection Directive. The Data Retention Directive and the Directive on Privacy an Electronic Communications will stay in force and supplement the Regulation as they have done it in the past with the Data Protection Directive.

4.4.2.2.2. Content of the Reform

The proposal for the European Data Protection Regulation contains the following key changes:

Scope

The regulation applies if the data controller or processor (organization) or the data subject (person) is based in the EU. Furthermore (and unlike the current Directive) the Regulation also applies to organizations based outside the European Union if they process personal data of EU residents. According to the European Commission "personal data is any information relating to an individual, whether it relates to his or her private, professional or public life. It can be anything from a name, a photo, an e-mail address, bank details, and posts on social networking websites, medical information, or a computer's IP address."

Single Set of Rules[22]

One single set of rules applies to all EU member states and there will be one Single Data Protection Authority (DPA) responsible for each company depending on where the Company is based or which DPA it chooses. With this 'one-stop-shop' application, companies in the EU will be answerable to a single data protection authority (DPA), no matter how many EU countries they do business in. A European Data Protection Board will coordinate the DPAs. Companies with more than 250 employees should be proactive and take measures to ensure compliance with data protection law by appointing a data protection officer. There is an exception for employee data that still might be subject to individual country regulations.

[22]European Commission: Factsheet on: How will the EU's data protection reform benefit for the European businesses?

Responsibility & Accountability
The notice requirements remain and are expanded. They must include the retention time for personal data and contact information for data controller and data protection officer. Data Protection Impact Assessments (Article 33) have to be conducted when specific risks occur to the rights and freedoms of data subjects. Risk assessment and mitigation is required and a prior approval of the DPA for high risks. Data Protection Officers (Articles 35-37) are to ensure compliance within organizations. They have to be appointed for all public authorities and for enterprises with more than 250 employees.

Privacy by Design and Default[23]

In order to track down technological dangers during an early stage, the Data Protection Regulation has integrated the concept of Privacy by Design and by Default (Article 23). It requires that data protection is designed into the development of business processes for products and services. In addition, the controller has to implement mechanisms for ensuring that, by default, only those personal data are processed which are necessary for each specific purpose of the processing.

Consent
Valid consent must be explicit for data collected and purposes data used (Article 7; defined in Article 4). Consent for children under 13 must be given by child's parent or custodian, and should be verifiable (Article 8). Data controllers must be able to prove "consent" (opt-in) and consent may be withdrawn.

Fines
The GDPR contains a severe fine system which imposes the following fines:

- Up to €250K or up to 0.5% of the annual global sales for intentionally or negligently not responding to requests by the data subject or the DPA;
- Up to €500K or up to 1% of annual global sales for intentionally or negligently not complying with GDPR;
- Up to €1,000K or up to 2% of annual global sales for intentionally or negligently not complying with specific GDPR regulations.

Right to be forgotten
Personal data has to be deleted when the individual withdraws consent or the data is no longer necessary and there is no legitimate reason for an organization to keep it. (Article 17)

Data Portability
A user shall be able to request a copy of personal data being processed in a format usable by this person and be able to transmit it electronically to another processing system. (Article 18)

International cooperation
To respond to these challenges, the Commission is proposing a system which will ensure a level of protection for data transferred out of the EU similar to that within the EU. This will include clear rules defining when EU law is applicable to companies or organisations established outside the EU, in particular by clarifying that whenever the organisation's activities are related to the offering of goods or services to EU individuals or to the monitoring of their behaviour, EU rules will apply. The Commission is proposing a streamlined procedure for so-called "adequacy decisions" that will allow

[23]Neil Hodge, The EU: Privacy by Design: in: In-house Perspective, Volume 8, Issue 2, April 2012.

the free flow of information between the EU and non-EU countries. An adequacy decision is an acknowledgement that a given non-EU country ensures an adequate level of data protection through its domestic law or international commitments. Such adequacy decisions will be taken at European level on the basis of explicit criteria which will also apply to police cooperation and criminal justice.

4.4.2.2.3. Discussion & Challenges

The proposal for the new regulation is not final yet and discussed controversially. Amendments have been proposed. The single set of rules and the removal of administrative requirements are supposed to save money. But critics point out some issues:

- The requirement to have a Data Protection Officer (DPO) in companies with more than 250 employees is new for many EU countries and criticized by some for its administrative burden. For other countries like Germany this is lowering the level of data protection since there is already a requirement for a DPO in smaller companies (in Germany > 9 employees).
- The breach notification to the authorities within 24 hours is considered very ambitious.
- The GDPR was developed with a focus on social networks and cloud providers, but did not consider requirements for handling employee data sufficiently.
- Data Portability is not seen as a key aspect for data protection, but more a functional requirement for social networks and cloud providers.
- Language and staffing challenges for the Data Protection Authorities (DPA):
    - Non-European companies might prefer the UK / Irish DPA because of the English language. This will require extensive resources in those countries.
    - EU citizen do no longer have a single DPA to contact for their concerns, but have to deal with the DPA the company chose. Communication problems due to foreign languages have to be expected.
- The new regulation conflicts with other non-European laws and regulations and practices (e.g. surveillance by governments). Companies in such countries should not be acceptable for processing EU personal data anymore.
- American companies fear the introduction of higher Data Protection standards with the new Data Protection Regulation of the EU. Therefore, EU-politicians are confronted with an increased lobbying activity of American companies in order to amend certain paragraphs of the Regulation. In addition, with the effectiveness of the Regulation, the Safe Harbour Agreement between the EU and the USA might become obsolete.
- Currently specific contents of the proposal are still under discussion, but the biggest challenge might be the implementation of the GDPR in practice:
    - The European Commission and DPAs have to provide sufficient resources and power to enforce the implementation and a unique level of data protection has to be agreed upon by all European DPAs since a different interpretation of the regulation might still lead to different levels of privacy.
    - The implementation of the EU GDPR will require comprehensive changes of business practices for companies that did not implement a comparable level of privacy until now (especially non-European companies handling EU personal data).
    - There is already a lack of privacy experts and knowledge as of today and new requirements might worsen the situation. Therefore education in data protection and privacy will be a critical factor for the success of the GDPR.

4.4.3. Other IoT European Projects views on Ethics and Privacy

Our understanding of ethics and privacy issues can be further complemented by the findings of other European projects operating in the field of the Internet of Things. The Activity Chain 5 of the IERC cluster[25], focusing on Governance, Privacy and Security issues, can be considered as the main channel of discussion over these topics between the different projects.

4.4.3.1. IOT-A

During the stakeholder workshop SW5 in Bled conducted as part of the IOT-A activities in the autumn of 2012, ethics and privacy issues as well were discussed amongst the stakeholders present.
This is a quick recap of some of the concerns discussed, taken from a preliminary report of this workshop by Rob van Kranenburg.

- Business views:
  - Collecting data is not enough, we also need to use it or benefit from it
  - Personal data may be more meaningful to operators than to the owners of that data (comparison, correlation with other data sets allows to see patterns, trends)
  - Liability issues: Who is responsible for malfunctions in a integrated environment with many different actors / vendors / partners involved
- Technical views:
  - Where does the intelligence / information about users reside
    - In each device, sensor
    - In bundling / orchestrating personal devices (e.g. mobile phones)
    - In a server
    - In the network, in the cloud
  - How much intelligence is needed in devices anyway, if they are supposed to be self-learning, adaptive, ambient
  - How can the following decisions be made easy (and understandable) for the user
    - What information / how much information do I want to share (do I have to share for the process to work)
    - Who may have access to this information (and the information derived from it)
    - How can I delete / change / control information that is out there
  - Can we “silence a chip” i.e. can transmission of data be controlled, stopped easily
  - Do we need to check devices coming onto an environment for “bad” data, viruses, other threats
- Broader Ethical and social views (Individuals and society)
  - What will happen to us as human beings, if all our environments are uniform and personalised? What effect will a lack of challenges have on us?
    - Boredom where thrills / excitement will be looked for outside (trends already existing today)
    - Stalled development of the human race, “zero creativity” (adaptation to the environment is one of the main drivers of evolution)
  - How will correlation of granular data affect the know-how about a person (Example: Hotels have info about personal preferences, by checking which hotel accessed this data and when, it will be possible to infer the travel itinerary of a person)

[25] http://www.internet-of-things-research.eu/activity_chains.htm

- How will the learning/adaptation of intelligent devices be guided. Who decides what is “good” knowledge and what is “bad”
- Who controls the morals of the network, how does the intelligent ambient network react if these moral standards are breached
- What if my guests (or hosts) load my preferences / personal data onto their devices, how and by whom will my data then be protected
- Serenity / feeling of safety vs. carelessness, over-reliance on devices (example: my oven shuts down automatically anyway, I don’t have to think about it)
- Ambient Living is supposed to make life easier, but might indeed put more stress on people, because people need to feel in control for their wellbeing (several psychological studies show this, add some links)

- Ideas for further analysis
  - Use the PIA (Privacy Impact Analysis) as a framework for individual use cases
    - In the case of BUTLER (or indeed ambient living) it is not so easy to determine individual use cases
    - Scenarios need a deep understanding not only of functionality, but also of context and user preferences
  - Is there a “right to forget”, how could that be enforced

Conclusion:

The environment of the Internet if Things will be heterogeneous; a green field “one size fits all” approach is completely out of the question. So middleware is a necessity.

But middleware / interfaces / standards are not just technical issues they are also a social and cultural issues. Knowledge about users and preferences might become a service layer.

4.4.3.2. iCore[26]

The iCore cognitive framework is based on the principle that any real world object and any digital object that is available, accessible, observable or controllable can have a virtual representation in the “Internet of Things”, which is called Virtual Object (VO).

The virtual objects (VOs) are primarily targeted to the abstraction of technological heterogeneity and include semantic description of functionality that enables situation-aware selection and use of objects. Composite virtual objects (CVOs) use the services of virtual objects. A CVO is a cognitive mash-up of semantically interoperable VOs that renders services in accordance with the user/stakeholder perspectives and the application requirements.

The overall layered approach of the iCore project is provided in Figure 16:

[26] The following section is an extract from the AC5 chapter of the IERC 2013 book on the Internet of Things.

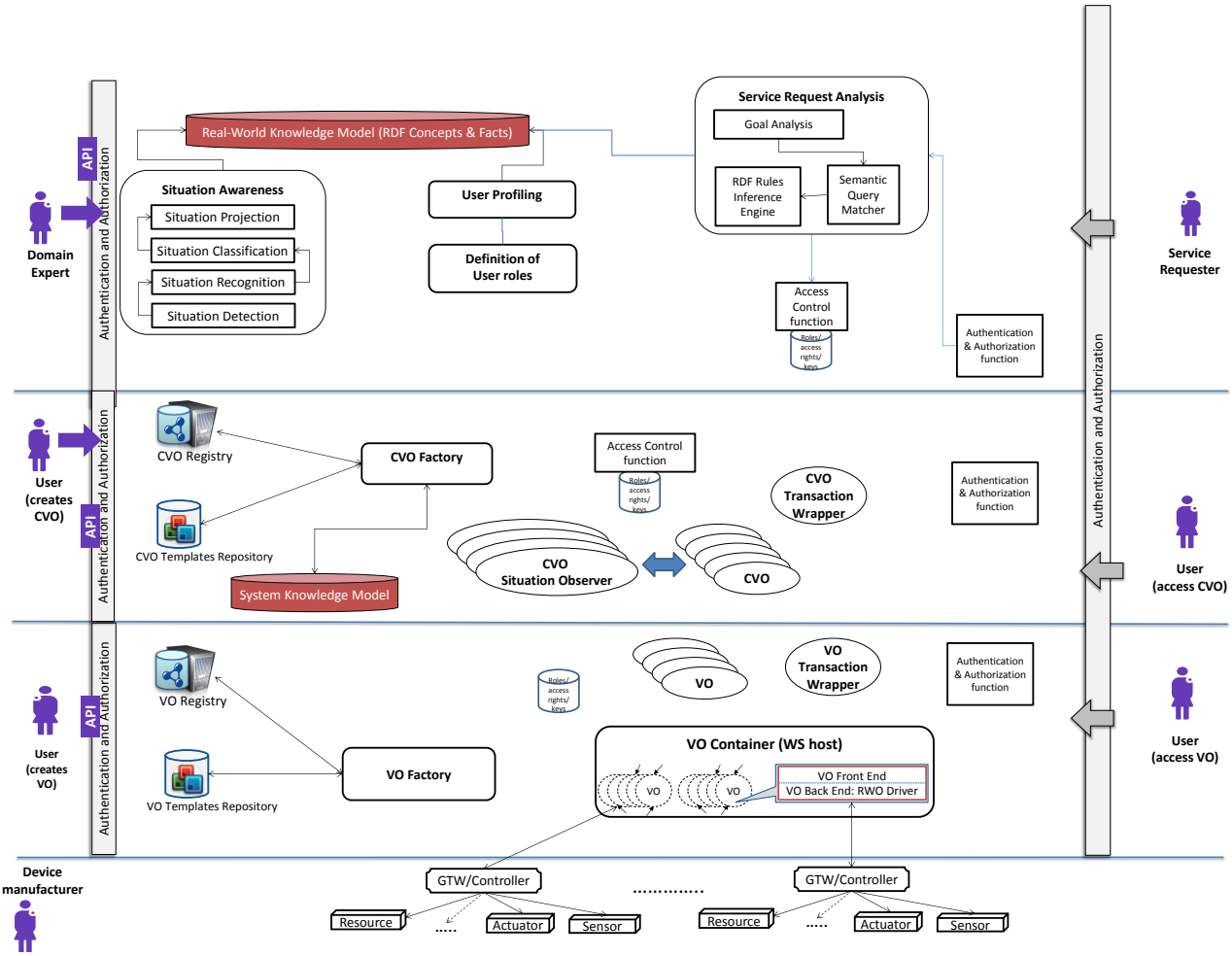


Figure 16 - iCore framework

The first cognitive management layer (VO level cognitive framework) is responsible for managing the VOs throughout their lifecycle, ensuring reliability of the link to the real world object / entity (e.g., sensors, actuators, devices, etc.) they represent.

The second cognitive management layer (CVO level cognitive framework) is responsible for composing the VOs in Composite VO. CVOs will be using the services of VO to compose more sophisticated objects.

The third level (User level cognitive framework) is responsible for interaction with User/stakeholders. The cognitive management frameworks will record the user's needs and requirements (e.g., human intentions) by collecting and analyzing the user profiles, stakeholders contracts (e.g., Service Level Agreements) and will create / activate relevant VO/CVOs on behalf of the users.

Governance, Security and Privacy in iCore is based on the following elements:

1) The access to data, resources (e.g. bandwidth or processing power) and services is regulated through a distributed access control model. Each VO/CVO and services has a specific level of access. iCore proposes an approach based on the sticky policy management approach. The underlying notion behind Sticky Policy is that the policy applicable to a piece of data (e.g. VO) travels with it and is enforceable at every point it is used. Users will therefore be able to declare privacy statements defining when, how and to what extent their personal information (also stored in a VO) can be disclosed. From an implementation point of view, the access control functions can be implemented by encrypting VOs/CVOs and by regulating the access to services in a specific iCore domain. In distributed iCore domains, access control requires distributed key management models, which the conditions that keys are never

distributed to the end users, which must be authenticated and authorized to use the iCore framework.

2) Users (i.e. a user can be a person or an application) must be authenticated and authorized to access the iCore framework and the related resources (i.e., VO, CVO and services). When a user is authorized, an access level is granted to the user and this information is recorded in the iCore framework. Access levels and relationships to users profile are defined by domain managers. Security mediation can be defined with authentication/authorization proprietary systems.
3) Policies can also be defined by domain mangers to implement specific rules (e.g., a product can be only bought on specific conditions). These rules can represent government regulations or business contracts.
4) Some of the systemic iCore functions (e.g., key management) are distributed across domains and they are connected through trusted connections. Data and resources can be distributed across domains through un-trusted means, because they are protected through the sticky policies model.

5. State of the Art

In this section we present the state of the art in term of privacy and data protection solutions for Internet of Things use cases and applications. We review general principles of privacy such as the need of informed consent, the principles of minimal disclosure, and anonymization of data, and the MEESTAR model. We then present rapidly the main data protection techniques which are presented in more detail in BUTLER deliverable 2.1[27]

5.1. Principles of Privacy

5.1.1. Informed Consent

Informed consent is a term which originates in the medical environment and describes the fact that a person – such as a patient or a participant in a research study – has been fully informed about the benefits and risks of a medical procedure and has agreed on the medical procedure being undertaken on them.

An informed consent can be said to have been given based upon a clear appreciation and understanding of the facts, implications, and future consequences of an action. In order to give informed consent, the individual concerned must have adequate reasoning faculties and be in possession of all relevant facts at the time consent is given

Impairments to reasoning and judgment which may make it impossible for someone to give informed consent include such factors as basic intellectual or emotional immaturity, high levels of stress such as PTSD or as severe mental retardation, severe mental illness, intoxication, severe sleep deprivation, Alzheimer's disease, or being in a coma[28].

From the medical research community the discussion of informed consent and how it is related to the usage of personal data collected as part of the research as well as what rights and responsibilities informed consent once given might entail can be directly applied to probably most of the BUTLER use cases, where personal data will also be collected and archived and probably be made available to other parties.[29]

With regard to the BUTLER scenarios, some of the problems of informed consent are related to these specific issues, which will be examined in the following chapters. It is important to know, that these are just examples and by no means the full list of all possible issues.

The issue of informed consent of the user is especially important for the development of IoT, as the planned evolution of the European regulation (see section 4.4.2.2.2 above) is that "Whenever consent is required for data to be processed, it is clarified that it has to be given explicitly, rather than assumed"[30].

5.1.1.1. Information and Understanding

As stated above, informed consent needs to be given based on "clear appreciation and understanding of the facts, implications, and future consequences of an action"

[27] BUTLER Deliverable 2.1 : requirements, specifications and security technologies for IoT Complex Aware Applications available on http://www.iot-butler.eu/download/deliverables

[28] Definition and explanation taken from Wikipedia http://en.wikipedia.org/wiki/Informed_consent (last accessed February 4th, 2013)

[29] Corti, Louise; Day, Annette & Backhouse, Gill (2000): Confidentiality and Informed Consent: Issues for Consideration in the Preservation of and Provision of Access to Qualitative Data Archives [46 paragraphs]. Forum Qualitative Sozialforschung / Forum: Qualitative Social Research, 1(3), Art. 7, http://nbn-resolving.de/urn:nbn:de:0114-fqs000372.

[30] Press release: "Commission proposes a comprehensive reform of data protection rules to increase users' control of their data and to cut costs for businesses" http://europa.eu/rapid/press-release_IP-12-46_en.htm?locale=en

When BUTLER use cases evolve and more and more technical possibilities arise, what seemed unthinkable and impossible at the time the consent was given may very well become feasible and common. Say for example a person agrees to a monitoring and sharing of their movement data, to enable better control and perhaps steering of traffic flows for a municipality. The data of course will be stored and used anonymously, so it will not be possible to obtain a personal travelling profile from the data.

But let's assume that the person also signs up for automatic billing at the local chain of supermarkets, participates in a car-sharing community, where the person can book and use any available car parked nearby and uses their mobile device to participate in an online community giving tips to other community members e.g. on special deals or local hot spots.

By linking the credit card (or other payment information) obtainable from the supermarket and the car sharing community with the movement data obtained from the municipality and the car sharing community and the freely shared information in the online community, it will be possible to form a rather good personal movement protocol of our user and at least in smaller towns or by observing over a longer period of time even be possible to identify him or her personally.

And even if that person consented to the usage of their data in all individual cases, it is very doubtful, that they will have fully understood and anticipated how easily a combination of this data could be achieved and used to identify and personally monitor them.

5.1.1.2. Adequate Reasoning Facilities

As can be seen from the list of reservations above, a lot of people are not considered to be able to give informed consent at all.

This is especially awkward for all those BUTLER use cases, which fall under the general topic of Ambient Assisted Living (AAL), since those use cases aim at exactly those persons, which can be said to not possess adequate reasoning facilities.

Another large group of possible users not covered directly by informed consents are all minors, which may either be using BUTLER directly or at least be exposed to BUTLER use cases in any public building, their own homes or just by walking down a road.

And while the consent can of course be given on behalf of all these people by their legal guardians, the problem of clear appreciation of all facts and a understanding of future applications does not become easier, if one has to give consent for somebody else.

5.1.1.3. Timing Issues

As has been pointed out, informed consent originates in the medical profession and has mainly been used in situations, which are either short in duration (an operation, a treatment) or where at least a beginning and an end can be defined (medical research).

Applying this idea to BUTLER is therefore bound to be difficult – if not impossible – because BUTLER cannot be perceived as a defined activity restricted by time limits but instead is something that may last indefinitely and may change and evolve over time.

5.1.1.4. Conclusion

By just taking the three aspects in the above chapters into account, we think it can be shown, that while informed consent may be one important building block in solving ethical or privacy issues within BUTLER, it will by no means the one solution that fits all.

5.1.2. Minimal Disclosure Principle

*"At the basis of the exchange between enterprises and customers, there is the **principle of transparency**:*

Enterprises should publish their privacy policy stating which data are collected and for what purpose. Another important principle is the notion of minimal disclosure: enterprises should maintain only information necessary to provide the service for which it was collected".[31]

Or in short:

- **Necessity**: Collect only that data you need for a service
- **Transparency**: Be open about what data you collect and for what purpose

These two premises form the basis for the minimal disclosure principal, and have been incorporated in basically all European data privacy acts.

So it seems sensible to analyze these two premises in the context of BUTLER and see, how they can be applied and where pitfalls and problems may arise.

5.1.2.1. Necessity

At a first glance, there seem to be no obvious problems with this rule. Of course enterprises and service organizations should not collect data, which they do not need.

But even leaving aside issues like data brokerage (cp. 5.1.4), this is not as simple as it seems.

BUTLER aims at delivering a "learning", self-adapting platform, which will predetermine future needs or user actions and will strive to become an increasingly important part of a user's life.

Or in the words of the BUTLER Document of work "*implement a well-defined vision of secure, pervasive and context-aware IoT where … the network reactions to users are adjusted to their needs (learned and monitored in real time)*"

If the system is truly to deliver on this promise, then more data will have to be collected, than is of immediate necessity, just in case the data should be needed at a later stage.

Let's look at an example:

- To perform assistance in looking for a well-situated and not too expensive parking place, the system will obviously at least need to know about
  - a user's final destination i.e. where the parking place should ideally be
  - the estimated time of arrival i.e. when the parking place needs to be available
  - the estimated time of staying in that parking place i.e. the time the parking place needs to be available for as well as the price to be paid for that time
- But a really clever system might sooner or later also want to know
  - the goals a user has at his or her destination, i.e. how close does the parking place really have to be. After all it will make a difference to the acceptability of the parking place location
    - whether the user wants to do the weekly grocery shopping, complete with carrying all those heavy bags
    - or whether the user wants to go jogging in the park anyway and will not mind those few extra steps
  - the current health situation of the user (or indeed all passengers in the car during a given trip) or some other personal information like age of the passengers, because it again may make a difference
    - whether a pram needs to be carried up a few steps
    - whether the passenger with the broken leg has to navigate with crutches on uneven ground

[31] Massacci, Mylopolous, Zannone. A Privacy Model to Support Minimal Disclosure in Virtual Organizations. Available at http://www.w3.org/2006/07/privacy-ws/papers/06-zannone-privacy-model/

- whether a bunch of school kids has to cross a busy road on their way to the cinema

So how exactly is “collecting only the necessary data” to be understood in this situation:

- Necessary for the service as it is implemented right now or for a service already anticipating future needs and services?

Of course one could always ask and inform the customer about collecting new data and what they are needed for right now. But as already discussed in chapter 5.1.1 on Informed Consent, that approach may also be difficult, especially since the possible customers we interviewed during our studies all indicated that “a lot of administration”, “dealing with the set-up of the system all the time” or “having to understand complex interdependencies” is not really what the customers want. They want their systems easy, useful and unobtrusive.

5.1.2.2. Transparency

As has already been said in the chapter above, the large majority of customers or users do not want to spend their precious time on setting up systems and thinking about privacy issues.

So how would a company or organization communicate the continuously evolving collection of user data and the changing uses this data is put to in a timely, open and yet non intrusive fashion.

So far the examples from say the social media are not encouraging; otherwise there wouldn’t be so many privacy scandals to read about almost every day.

One possibility as proposed by Massacci, Mylopolous, Zannone in their article on privacy and virtual organisations[32] and especially relevant here, because most BUTLER services will also be delivered through partnerships between different organisation is

- to decompose services into different combinations of sub-services according to their privacy threatening potential, using hypergraphs
- and to allow users to give privacy penalties to specific data sets
- and then automatically to decide through algorithms which combination of sub services best fits the customers privacy profile

An example of such a hypergraph can be seen in Figure 17.

[32]Massacci, Mylopolous, Zannone. A Privacy Model to Support Minimal Disclosure in Virtual Organizations. Available at http://www.w3.org/2006/07/privacy-ws/papers/06-zannone-privacy-model/

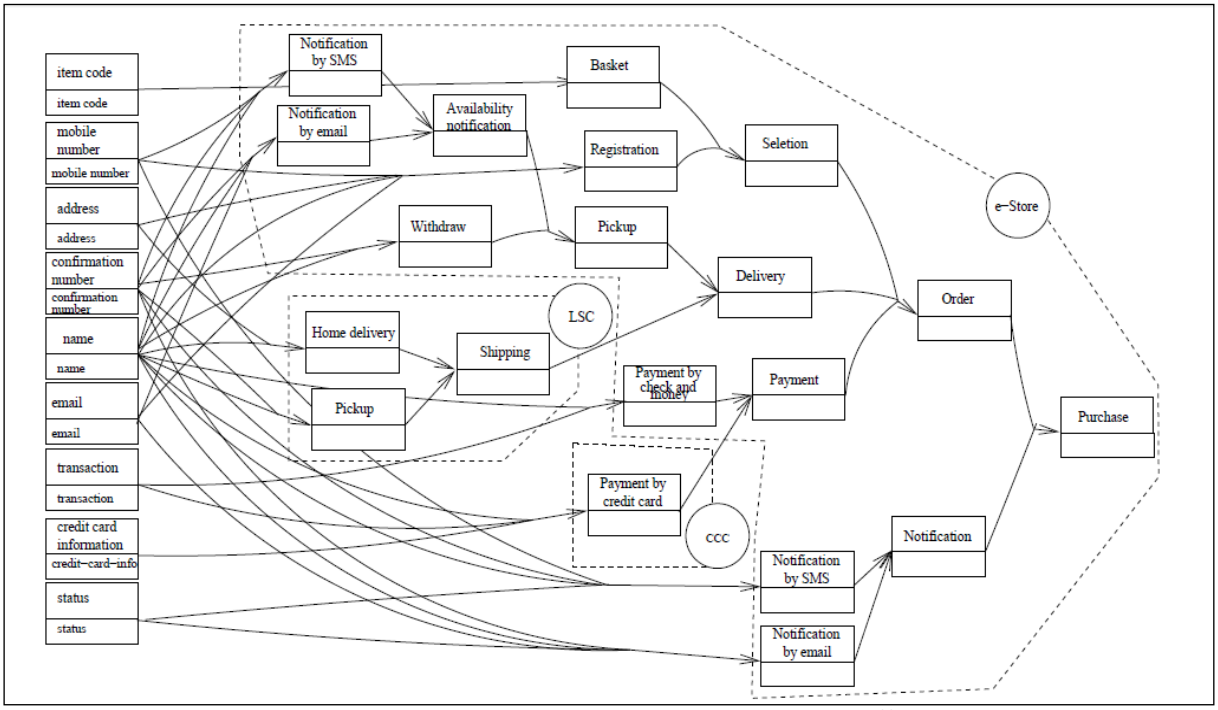


Figure 17 – Privacy Hypergraph for an Online Shop[33]

While this is a very thorough method of analysing privacy issues for a service and providing flexible transparency to a user, it also seems at least at a first glance to be rather complicated to understand and might be too much work for most users.

Especially since within an environment like BUTLER, different data sets might have different privacy penalties attached to them as far as the user is concerned. Because while it may be perfectly acceptable for a health service to collect and use data about blood pressure or blood sugar levels, the same data may carry a high privacy penalty if used by a shopping service.

5.1.3. Anonymisation of Personal Data

5.1.3.1. Definitions

As presented in the Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data[34], personally identifiable information (PII) can be defined as : “any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity”.

To protect the privacy of the data subject while processing the data or transferring the data to a third party, the concept of anonymisation of data and pseudonymisation of data have been developed[35]. Anonymisation, or pseudonymisation of data are being used whenever a set of potentially personal data is being delivered to a wider number of users, to enable them to study the data while at the same time aiming to preserve the anonymity and hence the privacy of the original

[33] Massacci, Mylopolous, Zannone. Ibid.

[34] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:NOT

[35] See: “Anonymity, Unlinkability, Undetectability, Unobservability, Pseudonymity, and Identity Management – A Consolidated Proposal for Terminology” by Andreas Pfitzmann and Marit Hansen, 2008 for detailed definitions of Anonymisation, Pseudonymisation and other identity management techniques. http://dud.inf.tu-dresden.de/literatur/Anon_Terminology_v0.31.pdf

data subjects. In order to make the data save for usage, the so-called PII or personally identifiable information is either being deleted (anonymisation) or replaced by neutral identifiers (pseudonymisation).

Paul Ohm describes this process of data anonymisation in his 2010 article in the UCLA Law Review[36]:

"*Now imagine that the office that maintains this database needs to place it in long-term storage or disclose it to a third party without compromising the privacy of the people tracked. To eliminate the privacy risk, the office will anonymize the data, consistent with contemporary, ubiquitous data-handling practices.*

First, it will delete personal identifiers like names and social security numbers. Second, it will modify other categories of information that act like identifiers in the particular context—the hospital will delete the names of next of kin, the school will excise student ID numbers, and the bank will obscure account numbers. What will remain is a best-of-both-worlds compromise: Analysts will still find the data useful, but unscrupulous marketers and malevolent identity thieves will find it impossible to identify the people tracked. Anonymization will calm regulators and keep critics at bay. Society will be able to turn its collective attention to other problems because technology will have solved this one. Anonymization ensures privacy."

5.1.3.2. The Failure of Anonymisation

But as has been shown again and again in the last few years, technology has by now made it possible to re-identify basically all anonymised data, making it easily possible to relate the data back to the individual persons it has been obtained from or indeed even to deduce information about individuals, whose original data did not even form part of the dataset as such:

- As early as 2000 Latanya Sweeney has proven that 87% of all Americans could be uniquely identified using only three pieces of information: ZIP code, birthdates, and sex[38].
- Researchers from the UNI Heidelberg published a study on social networks in 2012[39] proving that "*using machine learning one can reach a 85% prediction rate whether two non-members known by the same member of the social network are connected or not. Thus showing that the seemingly innocuous combination of knowledge of confirmed contacts between members on the one hand and their email contacts to non-members on the other hand provides enough information to deduce a substantial proportion of relationships between non-members.*"
- In a presentation given at the 9th European Trend Day on March 13, 2013 in Rueschlikon Valerie Casey pointed out that within an hour she was able to obtain databases with more than the necessary information to re-identify any set of anonymised data you might come across and the cost for these databases was almost negligible.

It is not hard to imagine that the advent of the Internet of Things, where even more personal data will be collected automatically and be made available for completely new functionality will make re-identification of data even easier than it already is today.

[36]Paul Ohm. Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization. UCLA Law Review, Vol. 57, p. 1701, 2010. Available at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1450006

[38] Nate Anderson. Anonymized data really isn't—and here's why not. September 2009. Available at http://arstechnica.com/tech-policy/2009/09/your-secrets-live-online-in-databases-of-ruin/

[39]Emöke-Ágnes Horvát, Michael Hanselmann, Fred A. Hamprecht, Katharina A. Zweig. One Plus One Makes Three (for Social Networks). April 2012. Available at http://www.plosone.org/article/info%3Adoi%2F10.1371%2Fjournal.pone.0034740#pone.0034740-Jernigan1

5.1.3.3. Possible Solutions

One seemingly obvious solution to this dilemma would be to further protect personal data by defining even more pieces as personally identifiable information (PII); but as Paul Ohm correctly points out:

"*Second, regulators can protect privacy in the face of easy re-identification only at great cost. Because the utility and privacy of data are intrinsically connected, no regulation can increase data privacy without also decreasing data utility. No useful database can ever be perfectly anonymous, and as the utility of data increases, the privacy decreases."*[40]

So instead, Paul Ohm suggests "*Faced with these daunting new challenges, regulators must find new ways to measure the risk to privacy in different contexts. They can no longer model privacy risks as a wholly scientific, mathematical exercise, but instead must embrace new models that take messier human factors like motive and trust into account."*

Paul Ohm then goes on to propose a list of *Five Factors for Assessing the Risk of Privacy Harm* in the last chapter of his article, in which he suggests to regulate access and usage of data according to the risk the data poses:

1. Data Handling Techniques as employed by the owners of the databases when letting others access the data
2. Private versus Public Release of data, because he argues that a private release to other trusted parties is much less likely to create harm then a public release of the same data
3. Quantity of data being released, because with the amount of data available the chances for re-identification rise
4. Motivations of the persons/organizations the data is released to, so researchers might be allowed access to different or more detailed data than commercial organizations
5. Trust, because if we can no longer trust the technology of anonymisation we should perhaps be able to trust the people who receive our data.

"*By applying the five factors, regulators will have a rough sense of the risk of re-identification of a particular type of provider in a particular context. If the risk is very low, regulators might choose to do nothing. If the risk is very high, regulators should feel inclined to act, imposing new restrictions on data collection, use, processing, or disclosure, and requiring specific data safe-handling procedures*.[41]"

A similar way of measuring the potential risk to privacy as well as other ethical issues is introduced in chapter 5.1.5 on the MEESTAR Model.

5.1.4. Limits of Data Protection with Regard to Data Brokerages

5.1.4.1. The Situation Today

In the words of the Federal Trade Commission whose motto after all is "Protecting America's Consumers" data brokers are "*companies that collect personal information about consumers from a variety of public and non-public sources and resell the information to other companies*.[42]"

In a privacy report, published in March 2012, the FTC set forth a voluntary framework of best practices for businesses based on the concepts of privacy by design, consumer control, and increased transparency for the collection and use of consumer data. This framework as proposed by the FTC is very similar to the content of the European Union's Data Protection Directive.

[40] Paul Ohm. Ibid.
[41] Paul Ohm. Ibid.
[42] Definition to be found on FTC website. Available at http://www.ftc.gov/opa/2012/12/databrokers.shtm

Both the Data Protection Directive and the FTC framework basically follow these OECD recommendations with regard to data collection[43]:

1. Notice—data subjects should be given notice when their data is being collected;
2. Purpose—data should only be used for the purpose stated and not for any other purposes;
3. Consent—data should not be disclosed without the data subject's consent;
4. Security—collected data should be kept secure from any potential abuses;
5. Disclosure—data subjects should be informed as to who is collecting their data;
6. Access—data subjects should be allowed to access their data and make corrections to any inaccurate data
7. Accountability—data subjects should have a method available to them to hold data collectors accountable for following the above principles.

This is already complex for many companies to achieve as well as difficult for a consumer to understand and take control of.

But as the same FTC report noted: while data brokers collect, maintain, and sell a wealth of information about consumers, they often do not interact directly with these consumers. Rather, they get information from public records and purchase information from other companies.

So the consumers have no idea who might be using their data and the data brokerages have no idea who the affected consumers actually are. And without a direct interaction between consumers and the data brokers, it becomes even more difficult - if not impossible - to guarantee adherence to almost all of the 7 principles listed above.

5.1.4.2. Further Complication with the IOT

The Internet of Things adds yet another dimension to the whole data brokerage topic, because with machine-to-machine communication and automatic data collection through sensors both in the public as well as in a private environment, consumers may not even realize anymore, that data is being collected at all, let alone, what kind of data, who is collecting it and what will happen to it.

For data brokers who then collect and analyze this kind of machine- or sensor-generated data, it therefore becomes completely impossible to adhere to any of the data privacy principles as listed above, because if the consumers do not know their data is being collected and there is no interaction between consumers and data brokers, none of these principles will work.

Of course one might argue that because the profiles generated by data brokers are anonymous, the privacy rights of individual consumers are still maintained. But as discussed in chapter 5.1.3, anonymisation of data has its own pitfalls and does no longer work properly as well.

5.1.5. The MEESTAR Model

5.1.5.1. Short Summary of the Study

The MEESTAR Model has been developed as part of a study on AAL (Ambient Assistant Living), its advantages and disadvantages and its social and economic impacts[44].MEESTAR stands for Model for the Ethical Evaluation of Socio-Technological ARrrangements (**M**odell zur**e**thischen**E**valuation **s**ozio-**t**echnischer **Ar**rangements) and is a model to analyse the ethical impact of technological invention, especially that of AAL systems.

In this analysis MEESTAR concentrates on the negative or at best neutral impact of technology, because its main aim is to identify and if possibly nullify possible harm as a result of the technology.

[43]Recommendations of the Council Concerning Guidelines Governing the Protection of Privacy and Trans-Border Flows of Personal Data.Available at http://www.oecd.org/document/18/0,2340,en_2649_34255_1815186_1_1_1_1,00.html

[44]A.Manzeschke, K.Weber, E.Rother, H.Fangerau. Ethische Fragen im Bereich Altersgerechter Assistenzsysteme. München, Januar 2013

MEESTAR does not try to evaluate a potential benefit, because the idea behind MEESTAR is, that it is not possible to compensate the negative ethical aspects with potential benefits.

To do the actual analysis, the MEESTAR model proposes a set of questions, where the answers are evaluated according to three dimensions, as can be seen in the following figure.

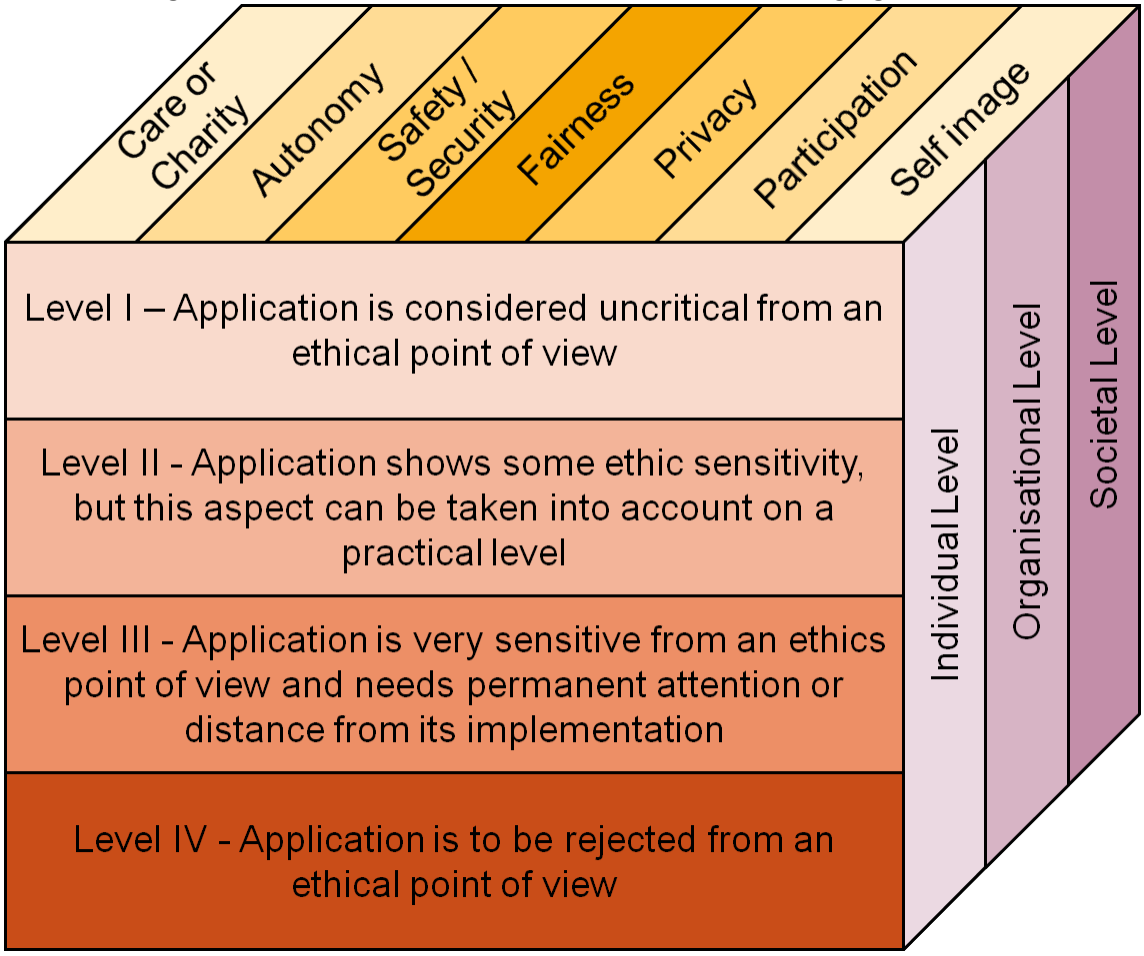


Figure 18: The MEESTAR model

The three dimensions are formed by

- Seven ethical aspects which have been identified as most relevant for AAL during the study (shown on the top or x-axis)
  - Care or Charity (Fürsorge)
  - Autonomy (Selbstbestimmung)
  - Safety or Security (Sicherheit)
  - Fairness (Gerechtigkeit)
  - Privacy (Privatheit)
  - Participation (Teilhabe)
  - Self-Image (Selbstverständnis)
- Four stages of ethical sensitivity (shown in front or on the y-axis) reaching from stage 1 (ethically unobjectionable) to stage 4 (from an ethical perspective unacceptable)
- Three possible viewpoints, from the personal, organisational or societal level

The authors of the study then propose to evaluate the answers to questions like the following in multidisciplinary workshops.

- Is the adoption of a specific AAL system ethically questionable or non-critical

- What can be done to minimise or neutralise the ethical problem, what solutions are there (both technical and organisational)
- Are there specific instances of using the system, which are that critical from an ethical point of view, that the whole system should not be installed
- Which aspects or functionalities of the system might be considered crucial from an ethical point of view and should be especially observed or monitored

Through this evaluation process, the authors hope to engender a spirit of ethical understanding in all parties involved in developing and using AAL systems and thus come to ethically acceptable solutions in an environment which due to its closeness and interwoven-ness with peoples' lives seems particularly prone to ethical dilemmas.

5.1.5.2. Applicability in a Broader IOT Context

The three dimensions the MEESTAR model proposes are in our opinion universally applicable to all sorts of ethical problems.

One might of course argue that there should be at least on additional stage of ethical sensitivity, which allows for positive impact on ethics, but this in our opinion not change the model fundamentally.

What is specifically tailored to AAL scenarios is the dimension of ethical aspects being considered. Especially the aspects of care and to a lesser extent those of self-image or participation are probably more closely related to AAL then to some of the other IOT scenarios.

Nevertheless, we think it would be possible to arrive at a similar set of ethical aspects for each IOT scenario – be it vertical or indeed as in the BUTLER case horizontal.

The main problem then seems to be, that MEESTAR does not actually deliver any answers, instead it is a tool aimed at analysis and asking questions.

But as we showed in some of the preceding chapters for example on Informed Consent, Minimal Disclosure Principle or Anonymisation of Personal Data, none of the technical or indeed legal answers given so far have been adequate to the ethical problems raised by the use of the technology.

5.2. Data protection techniques

Data technical protection mechanisms include two major aspects. One is the protection of the data at data storage, the other one the protection of the data at communication level. The protection of data at communication level is one the major area of research. Many communication protocols implement high level of end-to-end security including authentication, integrity and confidentiality either relying on symmetric cryptography algorithms; asymmetric cryptography like RSA, Elliptic Curves... and new incoming Identity Based Cryptography.

At communication level, the major issue is the deployment process of the security keys and the cost of the required hardware and software environment to run the security algorithms in efficient and secure way. One may rely on existing security key deployments – for instance a Service Provider may rely on Mobile Network Operator security application, but, in this case, such Service Provider shall have a commercial contract with the network operator and the technical implementation shall be complaint to required technical protocol (like GBA). This may be difficult and/or too costly compared to the revenue expected by the added security.

An exhaustive study of the communication protocols is available in "D2.1 Requirements, Specification and Security Technologies for IoT Context-aware network".

Privacy and Security do not only refer to security of the exchange of data over the network, but refer also to the accuracy of the data, either the keys involves in the secure protocol and/or the data themselves (personal identity, billing information). At client side, since few decades, smart card is known as a client security module. Nevertheless, the smart card can be attacked and smart card

constructors have different approaches to resist to attack. Anybody is able to build smart card operating system and integrate open source cryptographic algorithms, anyway, only few constructors provides secure implementation of operating system and algorithms able to resist to attacks which is a moving world.

Privacy and Security refers also to the security and protection of the server information. Payment Card Industry (PCI) – Security Standards Council https://www.pcisecuritystandards.org/ has developed of set of security standards. According to the server security, PCI-DSS 2.0 is the most relevant standard for solution involving financial information. In the Financial Industry parlance, *cardholder data* is data own by the holder of a credit card. For BUTLER, we extend the notion *cardholder data* to *personal data.* At server side, the keys involved in the security protocols shall be protected. Hardware Security Module is the most common equipment. Typical usage of the HSM is key derivation in symmetric cryptography. At server side, database shall be secure. Any major database providers (Oracle, Microsoft SQL server, IBM DB2…) have different products addressing the security requirements that shall be endorsed by the application.

Protection of the usage of the data

Once the personal data are protected at data storage and over the network, the usage of personal data shall also be protected. User may (or not) authorize applications to use its personal data. To implement this, application shall get access authorization, and retrieve the data on behalf of the user – so with its authorization. The authorization process is a dynamic notion – user may authorize an application to access its personal data, may remove this authorization, etc... In consequence, the entity providing the resource cannot encompass all the security information related to accessing entities. Therefore, the communication protocol shall support end-to-end security and also dynamic authorization mechanism. For this purpose, the protocol oauth-2.0is well suited at design level.

The oauth 2.0 security roles are: user, resource consumer – an application requiring access to a resource, resource provider – an entity returning a protected resource and authorization server – an entity managing the authorization on behalf of the user. The protocol works as follow:

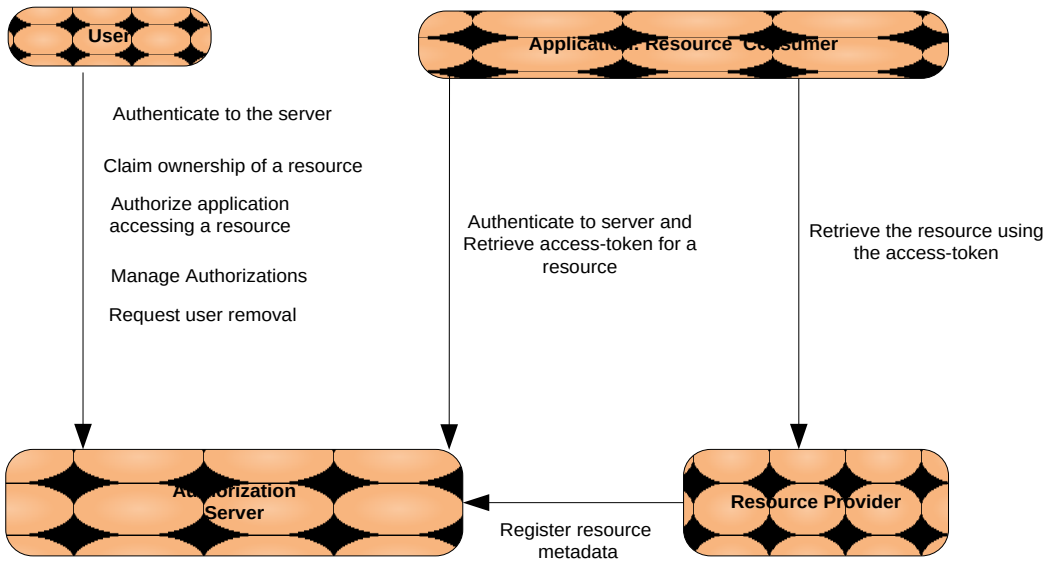


Figure 19 - Interaction between security roles

The above figure presents the interactions between Security Roles. A typical use case can be represented as follow:

1. Resource Provider registers a resource metadata to Authorization Server
2. User requires a service to an application – Resource Consumer.
3. Application connects the Authorization Server and retrieves a resource access-token on behalf of an authenticated user.
4. The application retrieves the protected resource and provides the related service.

Selective Disclosure of data.

In some circumstances, the user may select data he/she accepts to disclose to Resource Consumer; she/he can authorize only information computed from personal data. An example is the user identity and the corresponding age. Resource Provider may need to know if the user is 18-years old. Many techniques like Infocard, U-Prove, Idemix, Mera, support the selective-disclosure paradigm. Generally speaking, the mechanism follows the "claim based identity" paradigm. The claim based Identity logical mechanism permits implementation of Privacy where the returned data is computed according to the claims and do not encompass the complete user identity. For instance the returned data can expose only the age of the user – he/she is above 18 and no other user information. For instance the returned data can expose only the age of the user – he/she is above 18 and no other user information.

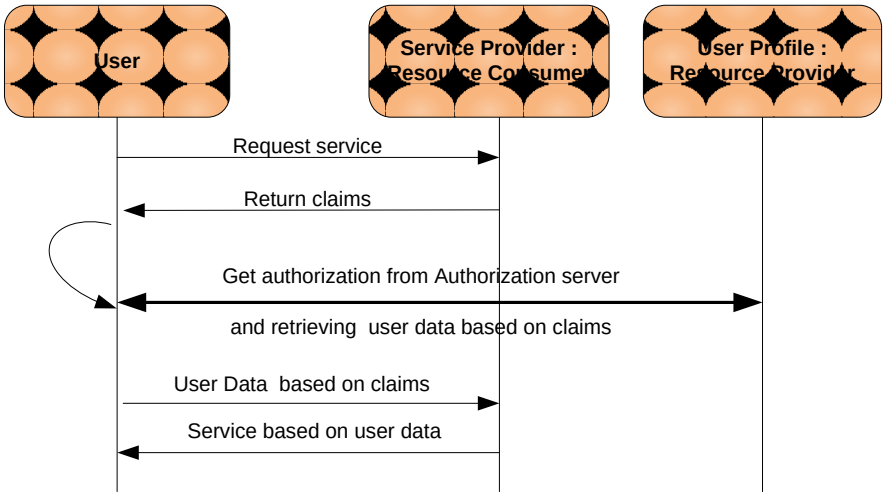


Figure 20 - Claim Based Identity

What cannot be solved?

The Data Protection techniques allow technical implementation of end-to-end security, authorization paradigm and selective disclosure. Anyway, for now, there is no technique to avoid misuse of fraudulent usage of collected personal data. Data mining techniques will be more and more powerful, at a time, user may think that disclosing data is not a problem according its privacy feeling; anyway, it could be a problem with new incoming techniques. To avoid this issue, the only solution is to follow the transparency principle.

> ***Transparency of usage of the data****: User – data subject in the European Union (EU) parlance - shall give explicit consent of usage of data.*

This principle implies that the user and the "resource consumer" have to define a contract including implicit or explicit declaration of the data usage. In consequence, each data shall follow a Data Policy that highlights how the data is managed. The policy shall answer, at least, to the following questions.

> ***Data Policy:***
> *- Why does the system need the data? It shall be for explicit reason.*
> *- What is the lifetime of the data?*
> *- How can the user access/control personal data?*
> *- to be completed ….*

6. Handling Privacy and Data Protection Issues in IoT

Based on the expectations identified in section 4 and on the state of the art done in section 5, this section propose different approaches to handle privacy and data protection issues in Internet of Things use cases. The approach proposed are broad and complementary: from the commitment to general principles for data protection, the privacy by design approach, the set up of technical solutions, and the important need for communication on privacy and data protection.

6.1. General principles on data collection, use and communication

The following general principles can give a first overview of policy to be applied to Internet of Things applications to reduce the risk of privacy breach:

- **Transparency of usage of the data**: User – data subject in the European Union (EU) parlance - shall give explicit consent of usage of data.
- **Collected Data shall be adequate, relevant and not excessive**: The data shall be collected on "need to know" principle. This principle is also known as "Data Minimization". The principle also helps to setup the user contract, to fulfil the data storage regulation and enhance the "Trust" paradigm.
- **Collector shall use data for explicit purpose**: Data shall be collected for legitimate reasons and shall be deleted (or anonymize) as soon as data is no longer relevant.
- **Collector shall protect data at communication level**: The Integrity of the information is important because modification of received information could have serious consequence for the overall system availability. User has accepted to disclose information to a specific system, not all the systems. The required level of protection depends on the data to be protected according the cost of the protection and the consequence of data disclosure to unauthorized systems.
- **Collector shall protect collected data at data storage:** User has accepted to disclose information to a specific system, not all the systems. It also could be mandatory to get infrastructure certification. The required level of protection depends on the data to be protected according the cost of the protection and the consequence of data disclosure to unauthorized systems. As example, user financial information can be used to perform automatic billing. Such data shall be carefully protected. Security keys at device side and server side are very exposed and shall be properly protected against hardware attacks.
- **Collector shall allow user to access / remove Personal Data**: Personal Data may be considered as a property of the user. User shall be able to verify correctness of the data and ask – if necessary – correction. Dynamic Personal Data – for instance home electricity consumption – shall also be available to the user for consultation. For static user identity, this principle is simply the application of current European regulations according access to user profile.

6.2. Privacy by Design approach

Privacy by design[45] is a framework that was developed by the Information and Privacy Commissioner of Ontario, Canada and that aims at integrating the handling of privacy concerns in the core of the technological innovation process.

The concept of Privacy by Design is built on the acknowledgment that:

- Privacy remains an important concern for end users, and a societal value to be safeguarded. The ignorance of privacy concern can be strongly damaging for organizations and businesses.

[45] http://www.privacybydesign.ca/

- Technological innovations can bring disruptions to privacy and create the condition of a "surveillance society"
- Reliance solely on regulations cannot ensure the protection of privacy.

The framework target three levels of applications:

- Information Technology: relying on the development and use of privacy enabling technologies (PET).
- Business practices: integrating the concern for privacy in the core of the business model and values of organizations.
- Physical design and infrastructures: integrating the concern for privacy in the design not only of information systems but in the physical assets and infrastructure that support them.

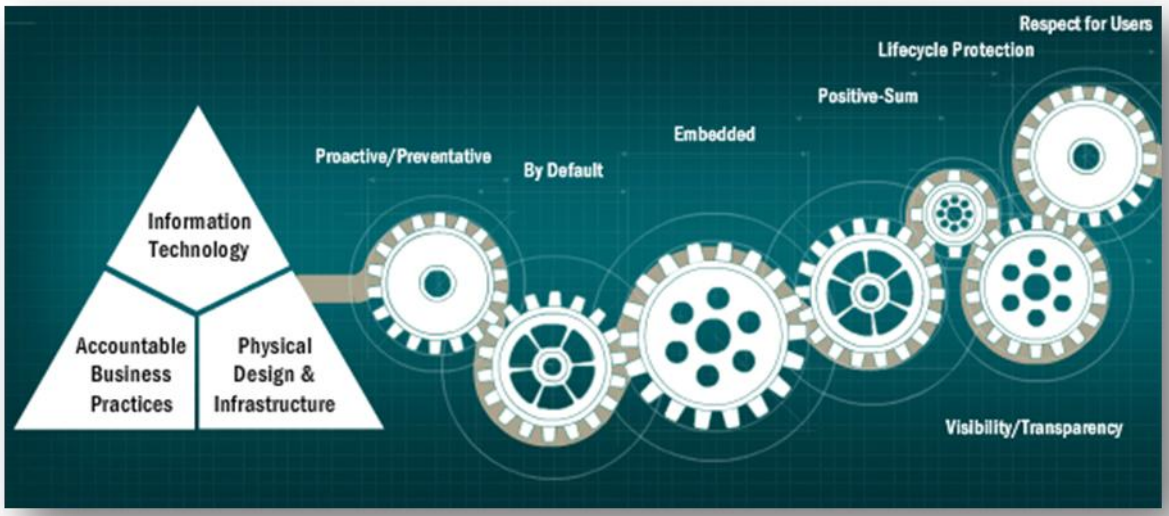


Figure 21 - Privacy by Design (source: www.privacybydesign.ca)

The framework recommends the application of 7 principles in the design or redesign of innovative technologies, services and applications:

- **Proactive and preventative** handling of privacy concerns that integrate threats to privacy of customers and users in the risk management process.
- Using privacy as the **"by default"** rule of any system or business practice.
- **Embedding privacy** in the design and architecture of IT systems and business practices.
- Ensuring that the protection of privacy is compatible with **full functionality** of the system or business practices and that no "trade-offs" are necessary to protect privacy.
- Protection of privacy throughout **the full lifecycle** of the service.
- Being **transparent and open** on the mechanisms involved and policy followed to safeguard privacy, in order to build trust.
- Adopt a **user-centric approach** that delivers privacy in a user-friendly way.

The framework also provides case studies and methodologies to apply the principles of "Privacy by Design" such as:

- A description of the application of the framework to the development and deployment of SmartMetering / Smart Grid solution in Ontario[46]

[46] http://www.privacybydesign.ca/content/uploads/2012/05/pbd-ieso.pdf

- Training materials to implement a "Privacy by Design" policy in an organization[47]
- Studies of the implementation of Privacy policies in biometric security applications[48]

An example of the principles of Privacy by Design put in practice in the field of the Internet of Things can be found in the Privacy and Data Protection Impact Assessment Framework for RFID Applications[49] created under the impulse of the European Commission[50].

The Impact Assessment Framework describes the step to be followed prior to any development and deployment of RFID technologies, to evaluate and address any related Privacy Concerns. The framework proposes a two phases process; in the first phase the analysis determines the type of analysis needed, in the second phase the analysis focuses on the privacy risks. This approach focuses on a detailed description of the proposed RFID application, with focus on an identification of privacy risks. Each risk shall then be addressed by appropriate controls and the processes as well as the results have to be monitored in a report.

The following figures present the two phases of the privacy impact assessment of RFID applications.

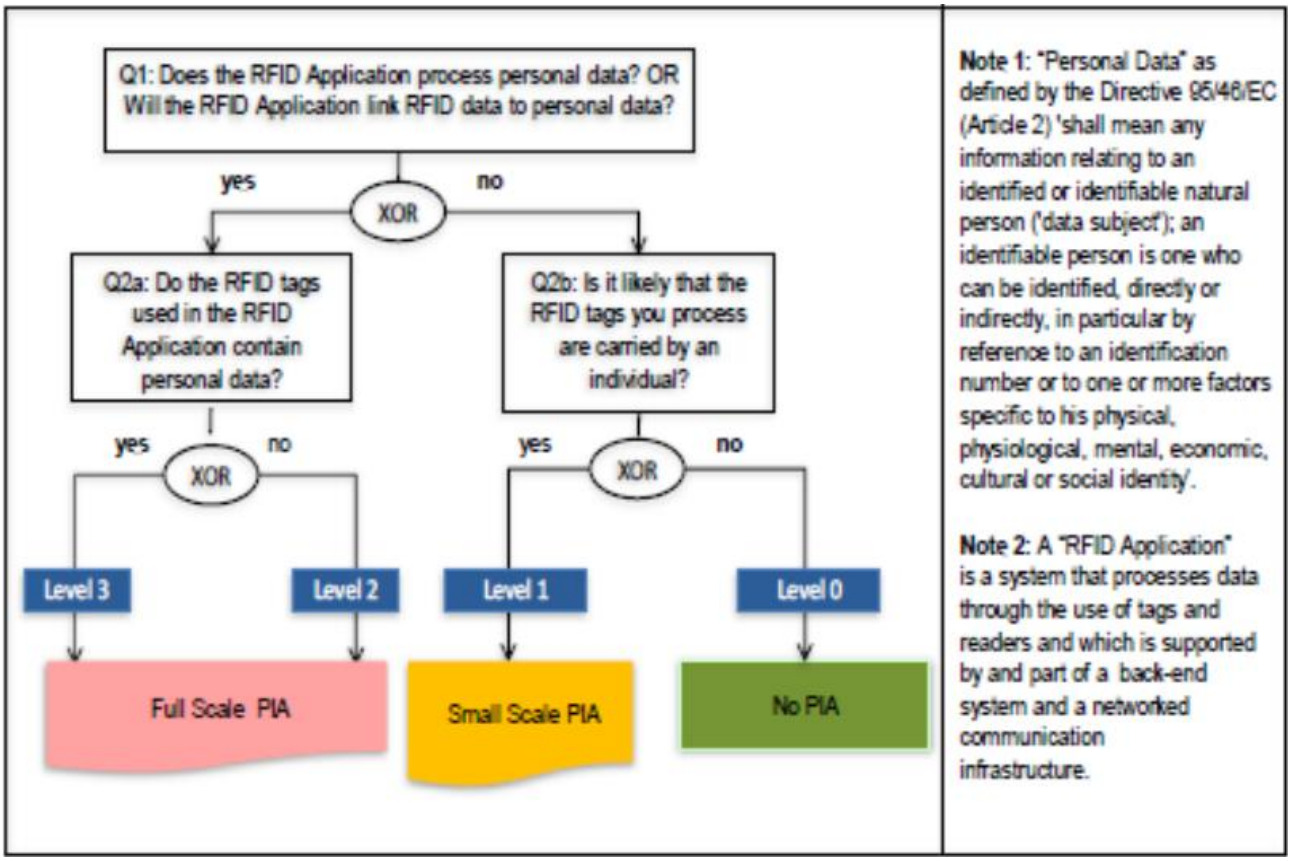


Figure 22 – RFID Privacy Impact Assessment Framework, phase 1 (source: http://cordis.europa.eu/fp7/ict/enet/documents/rfid-pia-framework-final.pdf).

[47] http://www.privacybydesign.ca/content/uploads/2013/01/operationalizing-pbd-guide.pdf

[48] Ann Cavoukian,"Advances in Biometric Encryption: An Example of Privacy by Design From Research to Proof of Concept" 2012 Digital Enlightenment Yearbook 2012http://ebooks.iospress.nl/publication/31988

[49] http://cordis.europa.eu/fp7/ict/enet/documents/rfid-pia-framework-final.pdf

[50] http://ec.europa.eu/digital-agenda/en/blog/the-privacy-and-data-protection-impact-assessment-framework-for-rfid-applications-a-defining-moment-in-the-modern-epic-of-co-regulation-in-ict#more-17

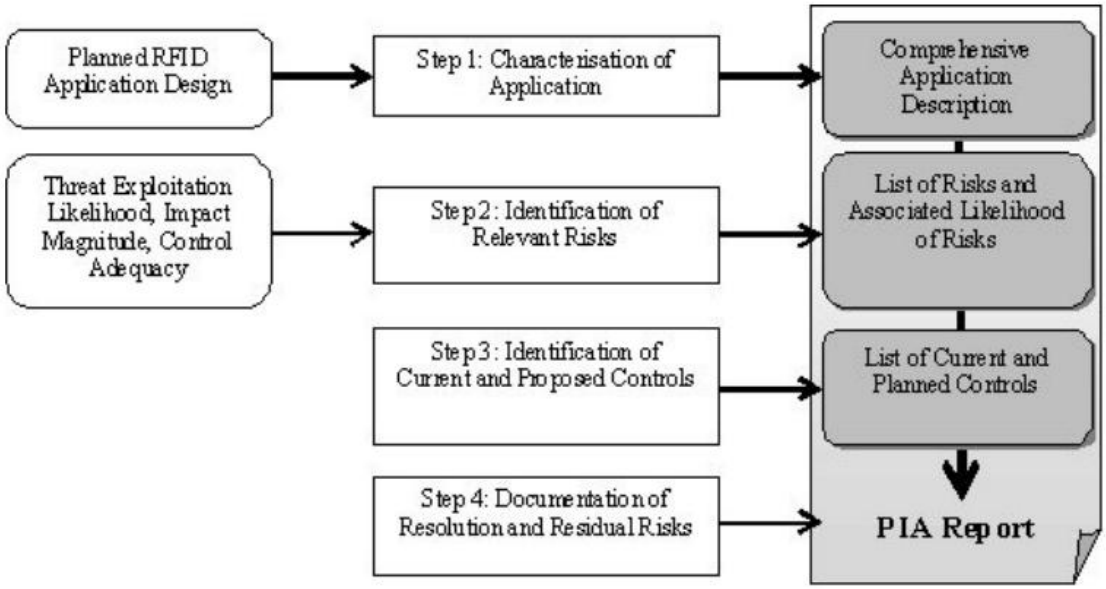


Figure 23 - RFID Privacy Impact Assessment, phase (source: http://cordis.europa.eu/fp7/ict/enet/documents/rfid-pia-framework-final.pdf).

To sum up, the "Privacy by Design" concept promotes the systematic questioning of ethics and privacy issues at every step of the design of a new service, starting as early as possible. Privacy is therefore seen as an ethics of knowledge[51,52] and treated as such.

6.3. Technical solution set up

The following technical solution set up is being developed in the scope of the BUTLER project to enable the "secure and privacy oriented" aspect of the BUTLER platform.

The abstraction of the BUTLER stakeholders highlights the concepts of **user, resource provider** and **resource consumer**. Users shall allow resource consumer accessing data from data provider**.** User shall be able to control the usage of its personal data which is also referred as protected resource. In horizontal scenario involving different stakeholders, user shall have a single point to manage the authorization to access its personal data which distributed among different Resource Providers; this single point is called the **authorization server.**

The BUTLER implementation relies on generalization of the authorization and resource concepts. To implement Privacy & Security principles, each entity in the BUTLER system shall implement one (or more) security roles.

Security Roles – definitions:

Role	Definition
User	User entity granting access to a resource. Generally, the user refers to a person, but can also refer to an application. The user shall be authorized to access the resource by the owner of the resource.
Resource Provider	Entity providing (and optionally updating) a resource. The Resource Provider

[51] Jeff Jarvis, "Public Parts; How Sharing in the Digital Age Improves the Way We Work and Live", 2011

[52] Data Protection Directive 95/46/EC - http://europa.eu/legislation_summaries/information_society/data_protection/l14012_en.htm and – http://ec.europa.eu/justice/data-protection/article-29/index_en.htm

	shall check an access-token to provide/update the resource. Resource Metadata shall be registered in Authorization Server (AS)
Resource Consumer	Client application getting and consuming resource on behalf of a user. Such user must be authorized to access the resource.
Authorization Server	The Authorization Server plays the role of Resource Directory. It implements access control management. The Authorization Server authenticates the user and authorizes resource-consumer getting resource by issuing a resource related access-token. Optionally, it may delegate the user authentication to an External Authentication Server
(optional) **Authentication Server**	This optional role can be used by Authorization Server to rely on authentication protocol not natively implemented in the Authorization Server. It means that the Authorization Server and Authentication Server shall federate some user identities.

Generic Access to Resource.

The following schema presents the overall message flow to access a protected resource. The access shall be authorized by the user.

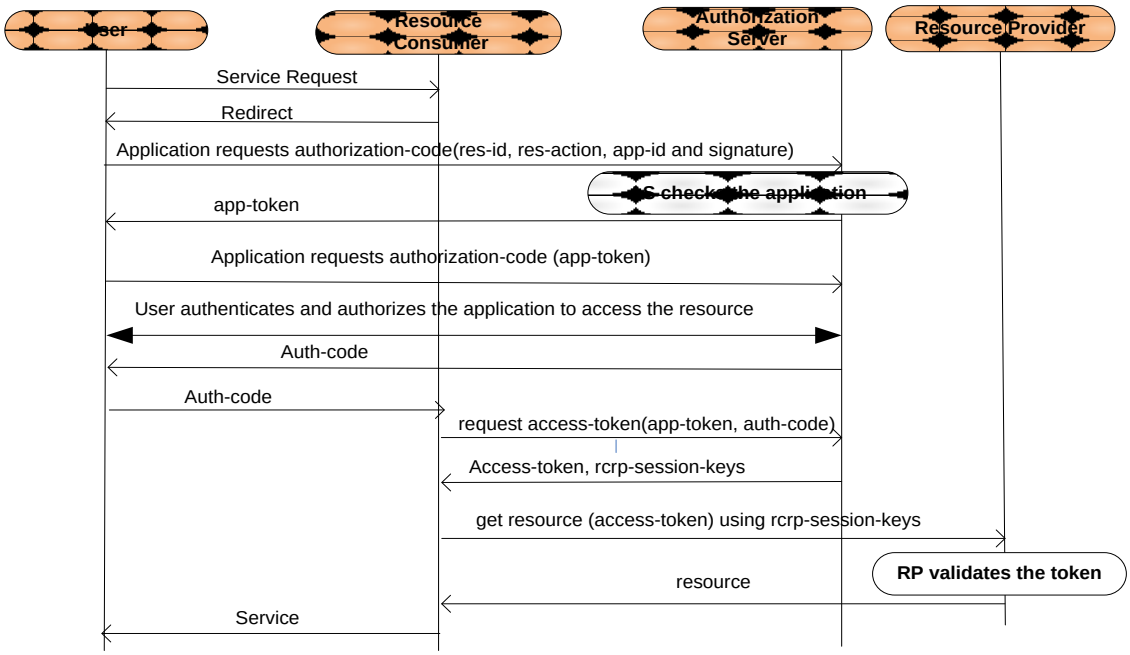


Figure 24 -Generic Access to Resource

The generic message flow is based on protocol OAuth 2.0.

The message flow is the following:

1. Using it user-agent, the user requests a service to a Service Provider. Here the Service Provider plays the role of Resource Consumer.

2. Through the user-agent, the application requests an *authorization-code* to access the resource. The Authorization Server checks the application and returns an *application-token*.
3. With the *application-token,* the application requests again an *authorization-code.*
4. The user authenticates to the Authorization Server and authorizes the application to access the required resource.
5. On behalf of the user – through the *authorization code* - the application requests the *access-token.*
6. The authorization server generates the *access-token* and randomly generated *rcrp-session-keys.*
7. Using the *access-token* and the *rcrp-session-keys,* the application requests the resource to the Resource Provider.
8. The Resource Provider checks the *access-token* and provides the resource protected by the *rcrp-sessions-keys.*
9. The application consumes the resource and provides the service.

NOTE: all the communications between the Resource Consumer and the Authorization Server and the communications between the User Agent and the Authorization Server rely on SSL protocol with Server Authentication. The Client Authentication is already implemented by the protocol OAUTH 2.0; therefore the communication between the Resource Consumer and the Authorization Server does not require SSL Client Authentication.

Resource Consumer / Resource Provider end to end security.

The resource is retrieved in a secure way. The protocol implements the following requirements:

- Application data is transported securely.
- The Resource Provider verifies that the *access-token* is a valid one.
- In case the *access-token* has been retrieved by a fraudulent application, the fraudulent application shall NOT be able to use it.

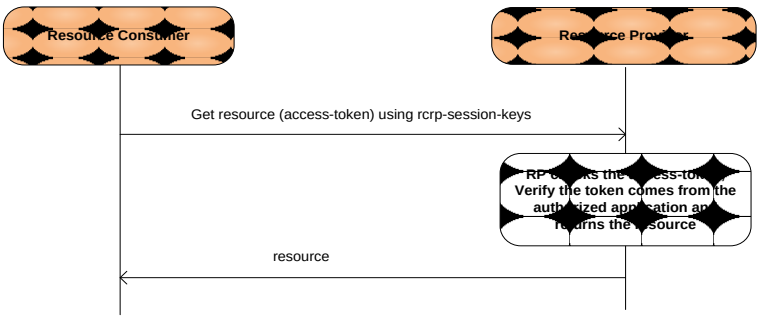


Figure 25 - Implementing End to end security

The BUTLER detailed architecture defines the security data and protocols involved in all the messages.

6.4. Communication and Information of user

Communicating and informing the user on the privacy and data protection policy of an IoT product, application or service is usually, to the very least, a necessity by legal obligations. Informing the user and keeping information available on the way private data are handled is a key component of the "informed consent" process (described above in section 5). And this principle is often, from a legal point of view, the founding principle under which the data gathering, analysis and exchange necessary for IoT application can happen.

However, the legal obligation of user information is by no mean sufficient to guarantee that the information provided is actually understandable by the majority of users, or even that the users will actually access this information. The technical and legal complexity, specificity, and changing nature of IoT application and data protection principles can be a strong limitation to the actual understanding of the end-user in an "informed consent" decision. The number of data collection and use operation made by IoT applications, and the potential number of IoT applications that a single user will be using in a real life scenario further make a restricted approach to "informed consent" unpractical. If a user has to validate every data collection / use operation he will most likely either refuse altogether to use the applications or systematically agree without really taking care / understanding what is at stake.

6.4.1. Privacy as a Business Model

Despite these limitations, IoT applications and service developers and providers will have a strong interest in informing, educating and communicating with their users/customers as the emergence of "privacy based" business model will bring a competitive advantage.

Integrating "privacy" in a business model rely on the analysis that privacy is a clear need of Internet of Things future end users. This "customer" need, presented in section 4.3, can be summed up in a business point of view by the fact that most customers, when presented with two offerings, on which the sole distinction is their respect for privacy, will choose the most privacy oriented one. A privacy oriented business model will therefore integrate this customer need in the offering to use it as a competitive advantage.

The first organisations to adequately answer to this customer need, without reducing too sharply any other advantage of the offering (such as functionalities, availability or price), will, if they can build a strong communication on it, benefit from rapid and important growth in both users and revenues. By classical market mechanisms, a competitive race will then follow; pushing competitors to increase their efficiency in privacy protection and the quality of their communication on the way data is gathered, stored and used.

The case for a "privacy" oriented business model is especially strong in the perspective of IoT as to be a real success, IoT depends strongly on the quantity of data collected and therefore on the trust and acceptance of end-users. Building on the need for privacy and providing privacy oriented applications and adequate information to the user will therefore increase acceptance and create the necessary trust in the service. Furthermore a virtuous circle can be initiated as in turn the economical interest of the service providers for ethics and privacy issues, becomes a guarantee for the user that his privacy will be respected.

On the other hand, ignoring altogether the privacy requirements of end users and treating privacy only as legal burden can only be a losing strategy in the long run. First because of the increasing over time, risk that a competitor will take advantage of an aspect that you neglect. Secondly because from an economic perspective respecting privacy legislation becomes a burden for which the organization have to pay without any competitive benefit. And finally because building a business on

ignorance and dissimulation, even ethics considerations aside, is usually not considered a wise choice in the long run and creating an IoT world without privacy would strongly imperil innovation[53].

To take advantage of the "privacy" asset, an organization would first have to integrate privacy in the conception and development of its offering (following for example the Privacy by Design framework). This can mean modification to the organization culture and decision process to integrate the privacy requirement in the hierarchy, become more transparent about the use of data and focus on user-centric privacy HMI design.

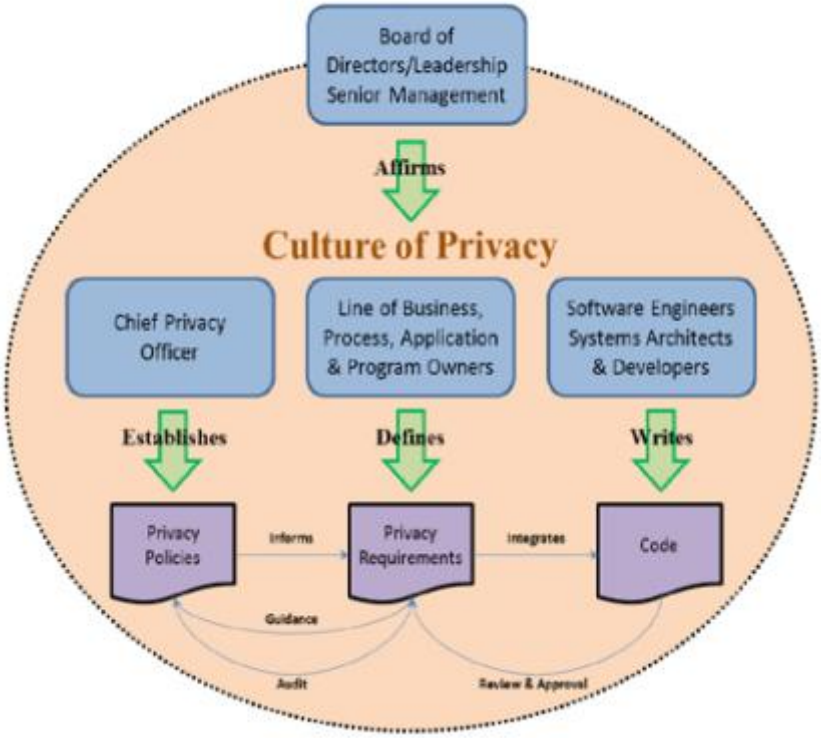


Figure 26 - Developing a culture of privacy in an organization (source: Privacy by Design)

But even more importantly, to really differentiate from competitors on privacy respect and data protection and initiate the privacy virtuous circle, the role of communication is essential. It is only by adequate, efficient communication on the potential ethic questions raised by IoT, and the implied need for privacy that an organization can differentiate, show the strength of its "privacy by design" approach and reap the benefits of its investment in privacy.

6.4.2. Communicating on IoT and Privacy

As seen above, organization developing and deploying IoT applications and services shall have a strong incentive not only to implement privacy protections but to efficiently communicate on it. Communication on privacy and IoT requires three key dialog elements:

- **Clear identification and explanation of the threat.** The competitive advantage of respecting privacy can only be achieved if the end users are aware of the risks. This can imply in the case of IoT explaining the identification possibility offered by large set of data and data mining techniques, or the redistribution of data.

[53] See "The Transparency Paradox: A Role for Privacy in Organizational Learning and Operational Control, Ethan S. Bernstein" above for the consequences of reduced privacy on innovation and productivity.

- **Transparent information on the way private data are handled by the organization.** Opening and publishing the methodology followed by the organization to external experts as well as concerned customers can be way to reinforce the perception of privacy protection.
- **Provide guidelines on how to use the services.** Ultimately the end user is often the sole responsible of the data he shares and a reasonable usage can help strongly to reduce privacy breaches. An organization should therefore provide best practices and user oriented guidelines on how to use its product and services, to ensure an efficient data protection policy.

This information should be:

- **Easily Available:** The information should be not only directly available for the user who looks for it but as much possible advertised to ensure the awareness of every user.
- **Clear and Understandable:** The privacy and ethics issues and the way they are managed must be presented in a clear and understandable way (avoiding technical or legal jargon) with the goal of educating the user.
- **Legally binding:** The declaration on the management of privacy and ethics must be legally binding for the service provider.
- **Consistent over time:** The way the ethics issues are managed, and the attached information shouldn't change without new notice to the user and these changes should be as few and rare as possible.

Setting up generic legal frameworks, along with dedicated easily identifiable logos or badges, for data collection, processing, use and sharing with third parties could be an interesting way to address the issue. Such an approach can be illustrated (in another field of application) by the creative commons policies and attached logos[54]. The use of logo enables rapid and accurate identification of the legal rights and policies in use and would ease understanding for the end user.

In addition and complement to communication by the organizations creating the Internet of Things services and applications, other stakeholders will participate to the communication on IoT privacy. Regulators as well as concerned user group have the same opportunity to launch communication campaign on the threats inherent to IoT applications, investigate the methodologies used to protect privacy, and provide best practices to reduce any remaining risk.

Finally a specific role can be identified for regulators in handling the truly ethics concerns raised by the transforming potential of IoT that are not directly privacy related, such as the risks of increased social (and knowledge) divides and loss of autonomy. These emerging issues and their potential impacts on society plead for real choices on the type of society that the citizens want, the underlying values and supporting imaginaries. Such decisions can hardly be imposed, but can emerge from a real and open public debate. The role of a democratic regulator would be to make possible and organize such a debate, and to implement the resulting vision in laws and education policy.

6.4.3. Integrating privacy by reputation systems

A complementary and promising approach to further increase end user information on privacy and data protection in IoT would be to rely on reputation systems.

As underlined by the Ethics factsheet[55] on the internet of things, "reputation systems such as can be found on Amazon, Slashdot or E-bay provide a possible technical solution to fulfil this condition by supplying sources of 'evidence' of behaviour or performance of other users as well as a reason for those users to live up that evidence as preservation of their online reputation depends on it".

[54] http://creativecommons.org/choose/
[55] Ibid.

The respect for privacy and the data policy used could be integrated in the ranking of the applications and nodes of the IoT. This ranking could not only provide information for end user but also be taken into account in automatic selection of which node are trustworthy for information sharing. Initial examples[56&57] of reputation based systems for trustworthy communications exists and could be extended and generalized to both become visible to end users and integrate user feedbacks and perceptions on IoT applications respect for privacy.

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

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

7. Privacy in BUTLER trial activities

In this section we present the activities and policy followed by the BUTLER consortium in the project experimentations (proof of concepts and field trials) regarding privacy, security and data protection. The main principles and legislation followed are presented, as well as the technical data protection mechanisms and the actual process used for protecting end users in Field Trials.

7.1. Acknowledgement of ethics, privacy and data protection issues in the BUTLER project

BUTLER project fully recognizes the need to ensure the end user privacy / security during the trials and the following section is devoted to this crucial topic.

We refer to Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. The Directive lays down a series of rights of the data subject. These are:

- The right of access to his / her personal data
- The right of erasure, blocking or rectification of the data, which do not comply, with the provisions of the Directive, are incomplete or inaccurate.
- The right to be informed of all relevant details relating to the data processing and the rights granted to him/her
- The right to a judicial remedy for any breach of the above mentioned rights.

As stated in the Seventh Framework Programme (Decision nª 1982/2006/EC), Article 6: "All the research activities carried out under the Seventh Framework Programme shall be carried out in compliance with fundamental ethical principles".

As already recognized in the Description of Work, BUTLER deals with a number of aspects that might impose ethical issues. Firstly, the project involves tracking the location of people, consumer behaviour modelling and user profiling. Moreover, focus groups will be created to receive feedback. Thus, the project raises ethical issues mainly related to data security and privacy. The awareness list presented in Annex C.1 "Project Awareness to Ethics and Privacy Issues" in the BUTLER Deliverable 1.2[58] presents in more details the issue raised by BUTLER and the responses envisioned.

As part of Work Package 1 (Use cases and requirements) and Work Package 6 (Exploitation), BUTLER not only considers ethical issues of the conducted research but also include considerations on ethical impact of the potential use of its research. The activity of the project has been presented in more detail above, in section 3.1.3, this chapter focuses on security mechanisms that are implemented in the BUTLER project activities that involve end users and examines how the user data will be handled in the project Proof of Concepts and Field Trials.

7.2. Security mechanisms within Proof of Concepts and Field Trials

Security and Privacy remain important characteristics of the BUTLER's Proof-of-Concepts. They include the security of the source of data, the accuracy of the data (personal identity, billing information), and the security of data exchange over the network (encryption keys and Smart Server's security). The implementation of privacy requirements may rely on security properties such as confidentiality, integrity, authentication and authorization. Confidentiality ensures that only the destination node can understand the message. Integrity ensures that the received message is the same transmitted by the source without modification during the transport phase. Authenticity

[58] BUTLER project deliverable 1.2 – Refined Trial Specification, available on www.iot-butler.eu/download/deliverables

certifies that the received message was really sent by the correct sender. An authority can verify that a node has the authorization to do some operations within the network. In fact, authorization specifies the access rights to resources. Availability ensures that the network continuously operates as expected. Non-repudiation avoids that a node maliciously declares that it did not receive a message.

There is a need to restrict the access to any information available within the BUTLER system that intrinsically collects discrete data about users. The users' profile must be securely stored and transferred, and any access to it by an application must be monitored and controlled. Thus it is important to authenticate, authorize and account users for accessing data sensed by smart objects. Privacy needs to be also taken into account as users may not disclose their personal information stored in their profile. Authentication consists of assuring the authenticity of each interlocutor involved in the communication process. Users' authentication can be based on Login/password or PIN, software-based such as Facebook login, Fingerprint, SMS on users' phone, One Time Password or Smart Card. Once nodes authenticated and supplied their own secure communication channel, they can exchange confidential messages. Communications also need to be secured in order to avoid any wrong usage of data collected by the system. Cryptographic techniques are used to encrypt messages and ensure confidentiality (for example, based on TLS, etc.). Smart objects can take advantage of specific security feature included inside the communication standard they use (802.15.4, 6LoWPAN, ZigBee, COAP, ISA100.11a). Messages may also be signed in order to prove the senders' identity.

7.3. Privacy in the implementation and execution of field Trials

In preparing the pilot operations in proof of concepts and field trials, we will seek to guarantee the comfort and safety of participants and/or professionals who take part in them, as well as the security of their personal data (on preferences, profile and localization), acquired during the pilot evaluations.

This means in detail that:

- All the test subjects will have the ability to give informed written consent to participate (Annex D.1 "Letter of consent signed by field trial participants" in the D1.2).
- All the subjects will be strictly volunteers and are able to withdraw from the trials at any time without any restraints.
- All personal data collected during the Pilots on the subjects' preferences and habits will be strictly confidential.

In addition, all test volunteers, following detailed oral information, will receive:

- A commonly understandable written description of the project, the project objectives, and the planned project progress. (Annex C.2 – "Commonly understandable written description of the project" in the D1.2)
- The awareness list describing the procedures set forth by the project to guarantee their privacy in the course of the field trial. (Annex C.1 – "Project Awareness to Ethics and Privacy Issues" in the D1.2)
- Access to a complaints procedure. (Annex D.2 – "Complaint procedure information" in the D1.2)

Thus, the consortium shall implement the project in full respect of the legal and ethical national requirements and code of practice. Whenever authorizations have to be obtained from national bodies, those authorizations shall be considered as documents relevant to the project. Copies of all relevant authorizations will be submitted to the Commission prior to commencement of the relevant part of the project and will include in project periodic reports. Finally, Annex C.3 "Regulations

followed by the project to ensure data privacy" in the project Deliverable 1.2 (refined trial specifications) presents the individual situation for each partner regarding the data protection issue.

Summarizing, the following security and privacy measures are taken according to the field trial descriptions:

- Informed consent from all the involved end-users
- All personal information must be excluded from sharing
- Anonymising user data in the reported results
- Average and anonym data
- Datasets with max duration of 14 weeks
- Authentication of personnel and staff

All the field trial application operators will define the common policy for:

- information sensitivity measurement
- sharing and accessing information depending on sensitivity level

The implementation of the field trial policy in each field trial will be the responsibility of the trial organizer (a single organization by trial), All trials will be in depth reviewed by the task leader (iHomeLab) and by the project coordinator (inno) and quality manager (ERC) to ensure that the policy defined by the project is applied. Additionally the Quality Plan of the project (Deliverable 7.4) will be applied to field trial in the same way as any other project deliverable (implying review by independent reviewers), and the management of ethical risks has been integrated in the risk management process of the project (implying regular review in plenary / general assembly meetings).

Annex A Global Requirements and Constraints from D1.1

A.1 Global Non-Functional Requirements

A.1.1 Non Functional Requirements which Address Ethical Issues

Requirement ID	Description	Rationale	Use Case ID
Global_NFR_1	Users must be identified to use the system	Different topics like - access control - rights management - privacy management require the users to be identified and authenticated in all the locations / settings in which BUTLER might be active, e.g. - homes - restaurants and shops - transportation devices - public places	SmartCity_UC_2, SmartCity_UC_6, SmartCity_UC_8, SmartCity_UC_9, SmartCity_UC_10, SmartCity_UC_11, SmartCity_UC_15, SmartHealth_UC_9, SmartHealth_UC_10, SmartHome_UC_1, SmartHome_UC_4, SmartHome_UC_9, SmartHome_UC_13, SmartHome_UC_20, SmartTransportation_UC_3, SmartTransportation_UC_4, SmartTransportation_UC_7
Global_NFR_2	The consumer's authentication must be quick and simple.	Difficult authentication will not be suitable for usage for example in real shops or in any of the other situations / locations where a user must be authenticated.	SmartShopping_UC_2
Global_NFR_5	The system shall respect the privacy of users in all respects, for example: - when detecting a crowd, information about individual users shall not be gathered or accessed - preferences a user has selected are protected - services (such as alarms) a user subscribes to - queries a user puts to the system	Privacy control is one of the most important acceptance criteria for BUTLER.	SmartCity_UC_6, SmartCity_UC_7, SmartCity_UC_8, SmartCity_UC_9, SmartCity_UC_12, SmartCity_UC_15, SmartHealth_UC_3, SmartHome_UC_8, SmartHome_UC_9, SmartTransportation_UC_8

Requirement ID	Description	Rationale	Use Case ID
	- user profiles (containing sensitive and even non sensitive personal data) are protected - when monitoring a users behaviour the data gathered needs to be protected		
Global_NFR_6	The system shall take into account place & end-user privacy preferences, i.e. the user can decide - which data to share - when (in which situations) data will be shared - with whom data will be shared - which data the system can access - where (across which area) the data will be shared or accessible - whether shared data should be available anonymized or with personal information	Privacy control is one of the most important acceptance criteria for BUTLER. But in order for BUTLER to perform its "magic" a certain amount of data sharing between users is necessary and encouraged. So this data sharing must always be fully under the control of the user.	SmartCity_UC_15, SmartHealth_UC_6, SmartHealth_UC_3, SmartHealth_UC_8, SmartHome_UC_8, SmartHome_UC_15, SmartShopping_UC_1, SmartShopping_UC_2, SmartShopping_UC_3, SmartShopping_UC_4, SmartShopping_UC_5, SmartShopping_UC_6, SmartShopping_UC_7, SmartShopping_UC_8, SmartTransportation_UC_5, SmartTransportation_UC_6
Global_NFR_16	The system contains a role management, where - different users can have different roles - roles can be shared by users or groups of users - a user can have a different role with regard to different services within the system - access to certain	Some specific privileges should be granted for example to the owner of a place to define access control & privacy rules as well as to manage place embedded sensors.	SmartCity_UC_6, SmartCity_UC_8, SmartCity_UC_9, SmartCity_UC_15, SmartHealth_UC_1, SmartTransportation_UC_10, SmartTransportation_UC_8

Requirement ID	Description	Rationale	Use Case ID
	services can be restricted according to the roles a user has		
Global_NFR_17	the system shall be able to administrate different user levels	the system should have different levels for different person for example a doctor is able to see everything, a friend only restricted view etc.	SmartHealth_UC_1, SmartTransportation_UC_10
Global_NFR_21	The system shall allow the user to personalize his/her user profile	The users will personalize their profile in order to specify their preferences. Based on the nature of the user, this personalization can be different for different users.	SmartCity_UC_1, SmartCity_UC_3, SmartCity_UC_4
Global_NFR_22	The system shall enable the owner to set/create the applications proposed within his place.	It's up to the owner to decide which applications are relevant for his place. Locally-wised applications chosen by the owner himself would improve the experience of the places Addressed ethical concerns: Free will of the user / self determination of the individual is taken care of, by allowing the user to chose which services to use (or refuse)	SmartCity_UC_16
Global_NFR_24	The system shall be able to deliver reports or notifications to users or groups of users	On detecting problematic or illegal situations, the system will have to be able to notify the correct authorities Addressed ethical concerns: To a certain extent law enforcement abilities will be designed into the system from the beginning. Additional ethical concerns: Of course this in turn raises extra questions	SmartCity_UC_1, SmartCity_UC_3, SmartCity_UC_4, SmartTransportation_UC_7

Requirement ID	Description	Rationale	Use Case ID
		about privacy and self-determination that need to be considered carefully in this context.	

A.1.2 Non Functional Requirements which Raise Further Ethical Issues

Requirement ID	Description	Rationale	Use Case ID
Global_NFR_3	The system shall provide the means for the identification of the object associated with a user	For example in the SmartTransport environment: Guaranteeing that a given car is the one being driven by the user is a key functionality. Additional privacy concerns: The identification of such relations between objects and individuals need to be controlled and protected same as any other personal data.	SmartTransportation_UC_8
Global_NFR_4	The system shall identify and localize users / actors in a certain area	outdoor as well as indoor localization system should be provided in order to detect the accurate location for example of the volunteers on request Additional privacy concerns: The localisation of individuals needs to be controlled and protected same as any other personal data and it must be possible for individuals to hide their current location if they so desire.	SmartTransportation_UC_10, SmartCity_UC_15
Global_NFR_8	The system must be able to monitor individual objects, such as e.g. - specific streetlamps - water valves and actuators - vehicles and their occupants In order to do this, certain information about the objects must be known to the system e.g.	In order to control objects, the system needs to be able to monitor them first. The system also needs to be able to monitor services being executed on or with an object, such as e.g. assistance given to a vehicle Additional privacy concerns: Here as in NFR_3 it is important to protect individual users' data as soon as these users have a relationship to a specific object.	SmartCity_UC_5, SmartCity_UC_7, SmartTransportation_UC_2, SmartTransportation_UC_10

Requirement ID	Description	Rationale	Use Case ID
	- physical location of an object - status of the object (like full/empty, on/off, open/closed) - relation of the object to other objects or users		
Global_NFR_13	The system shall provide the users with several user interfaces, according to the individual needs and preferences of a user or the situation the user is in. Possible types of user interface are: - graphical user interfaces over all kind of devices (smart phones, tablet PCs, video screens, virtual reality glasses, touch screens etc.) - geographical representations of data like map representations) - audio interfaces, both for alarms/notifications and for interaction Please note: This list is not complete!	In order to allow all kinds of users to interact with the system and to ensure maximum usability, user interface design will be a crucial topic for BUTLER Additional privacy concerns: It is very important to BUTLER to design all interfaces and the communication between interfaces and the system in such a way, that data protection and privacy is always ensured. Other additional ethical concerns: In order to be usable by all members of the public the design of accessibly (barrier free) interfaces is of the utmost importance in BUTLER	SmartCity_UC_1, SmartCity_UC_3, SmartCity_UC_4, SmartCity_UC_7, SmartCity_UC_8, SmartCity_UC_9, SmartCity_UC_10, SmartHome_UC_5, SmartHome_UC_6, SmartTransportation_UC_1, SmartTransportation_UC_5, SmartTransportation_UC_6, SmartTransportation_UC_8, SmartTransportation_UC_9, SmartTransportation_UC_10

A.2 Global constraints

A.2.3 Constraints which Address Ethical Issues

Requirement ID	Description	Rationale	Use Case ID
Global_C_6	All communication shall be secured		SmartCity_UC_13
Global_C_10	It must be possible for non-registered users to make use of selected resources that are managed by the system.	Except under certain circumstances, non-registered users may use a parking space with the same rights than registered users. Addressed ethical concerns: There cannot be two classes of citizens, those with access to BUTLER and those without. Both user groups need to have the same basic rights to public offerings.	SmartCity_UC_1, SmartCity_UC_3, SmartCity_UC_4
Global_C_12	The system needs to be implemented with usability always in mind. - The human computer interaction with the system must be user friendly and appealing. - Messages from the system need to be easy to understand and act upon. They should be motivating to the user. - maintaining / updating information needs to be fast and easy for the user	The design of the user interface(s) is one of the key issues in BUTLER: Because users can have all levels of technical expertise and need to be able to interact with the system from remote, this is a critical issue Addressed concerns: In order to be usable by all members of the public the design of accessibly (barrier free) interfaces is of the utmost importance in BUTLER	SmartHealth_UC_3, SmartHome_UC_1, SmartHome_UC_3, SmartHome_UC_4, SmartHome_UC_8, SmartHome_UC_9, SmartHome_UC_10, SmartHome_UC_13, SmartHome_UC_21, SmartHome_UC_22, SmartHome_UC_23, SmartCity_UC_17
Global_C_14	Data shall be secured at all times within the system, i.e. - when being stored in the system - during communication	Users must be sure that only accepted data are sent to the services and that such data are not corrupted or tampered with. The system also needs to make sure, that users do	SmartCity_UC_17, SmartCity_UC_11, SmartCity_UC_2, SmartHome_UC_9, SmartHome_UC_23, SmartShopping_UC_1, SmartShopping_UC_2, SmartShopping_UC_3,

Requirement ID	Description	Rationale	Use Case ID
	between parts of the system - while the systems communicates with other systems - when being accessed by a user - while being entered into the system or in other words Information transferred between users and system and stored in the system must be protected so that it is not possible for a third party to gain access to any information that the user or system privacy policy has classified as confidential information.	not cheat while entering data into the system.	SmartShopping_UC_4, SmartShopping_UC_5, SmartShopping_UC_6, SmartShopping_UC_7, SmartShopping_UC_8, SmartTransportation_UC_3, SmartTransportation_UC_7, SmartTransportation_UC_3, SmartTransportation_UC_4, SmartTransportation_UC_5, SmartTransportation_UC_6
Global_C_15	Updating user devices with service specific application shall be secure	The device shall not be updated with corrupted application.	SmartCity_UC_17
Global_C_19	The system must use cheap (0.01 - 0.5 Euro) RFID or wireless sensors to detect which items were forgotten	The system should rely on non-invasive technology to increase comfort of use and reduce cost	SmartHome_UC_10

A.2.4 Constraints which Raise Further Ethical Issues

Requirement ID	Description	Rationale	Use Case ID
Global_C_5	The system must be able to communicate with - remote parts of the system (like sensors, cameras, microphones, screens etc.) - Other systems for example to collect data, raise alarms etc.	The system should be as flexible as possible with regard to communication, for example the user should not have to be physically connected to the system, and there must be means to access the system remotely. Additional privacy concerns: It is very important to BUTLER to	SmartCity_UC_1, SmartCity_UC_3, SmartCity_UC_4, SmartCity_UC_16, SmartCity_UC_2, SmartCity_UC_10, SmartCity_UC_11, SmartHome_UC_19, SmartTransportation_UC_3, SmartTransportation_UC_7,

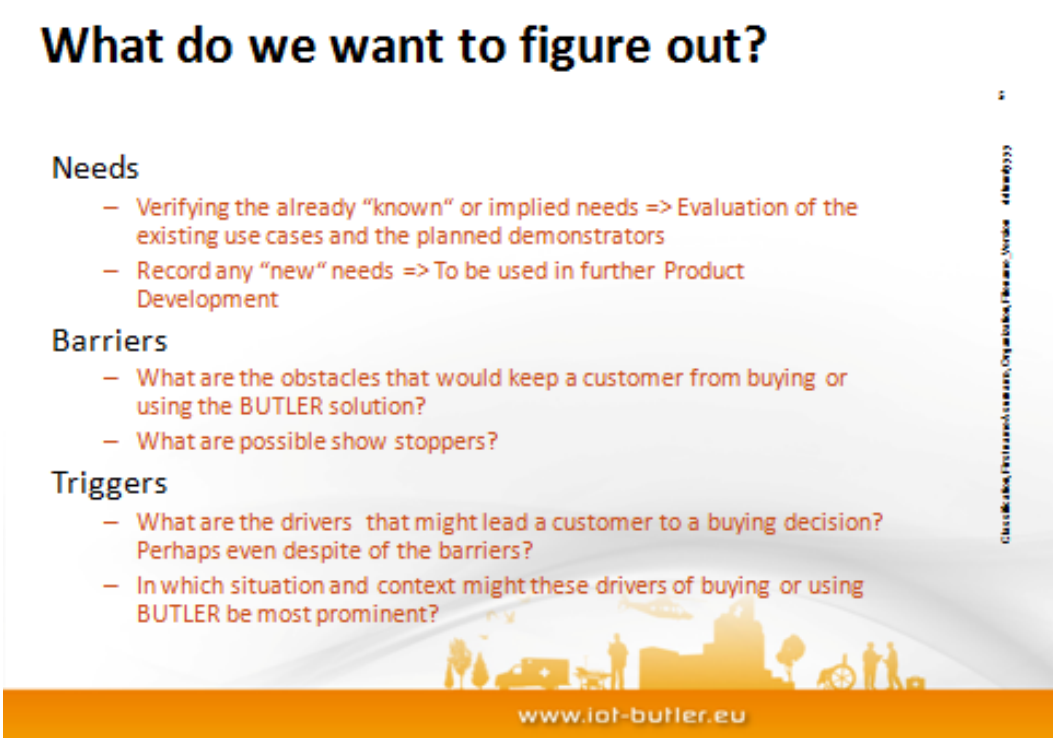
Requirement ID	Description	Rationale	Use Case ID
	- human recipients (registered and not registered users, administrators, control personnel etc.) For the communication both wired and wireless technologies can to be used, subject to specific needs and availability. Example from SmartCity: Sensor nodes deployed in a parking space will be often using wireless technologies to communicate with a gateway which will be often using both wired and wireless technologies. It is possible that a given communication will be executed in parallel via different mediums depending e.g. on the recipient or the location of the recipient. Example from Smart Transportation: Alarms about a traffic situation may be transmitted via wireless to authorities further away and through car to car communication to other users close by.	design the communication between all parts of the system in such a way, that data protection and privacy is always ensured. (see Global_C_6)	SmartTransportation_UC_9, SmartHome_UC_1, SmartHome_UC_4, SmartHealth_UC_9, SmartHome_UC_13
Global_C_7	The places should be equipped with network infrastructure elements that provide sufficient capabilities to allow for example real-time video streaming	A CCTV network or at least one camera should be deployed within the place (here the platform) to allow people to remotely check the situation. Additional privacy concerns: Access to any data collected by sensors, cameras or other machines that includes personal information will have to be protected by BUTLER at all times.	SmartTransportation_UC_5, SmartTransportation_UC_6
Global_C_8	The system needs to	For example the detection of a	SmartCity_UC_12

Requirement ID	Description	Rationale	Use Case ID
	be able to aggregate and correlate data from different sources to gain the correct information.	crowd is a difficult task that would benefit from the aggregation of several sources of information like usage of GSM antennas or streaming from the city cameras Additional privacy concerns: Access to aggregated and correlated data that might still allow to find out individual personal information will have to be protected by BUTLER at all times. Other additional ethical concerns: The system needs to make sure that information derived from aggregated or correlated data to predetermine user behaviour can be accessed and if necessary negated by the user.	

Annex B End User Interviews

B.1 Methodology

The following present the methodology followed by the end user interviews in the BUTLER project:



Target Group & Recruiting

Target group:

- Primarily aligned with the persona profiles (see materials)
- Gender split: Approx. 50% / 50% female / male
- Age: various generation representatives
- Education / Occupation: no IT professionals preferred
- good balance between academics and non-academics and between affluent and mid-level household
- Technical Know How: good balance between technical knowledgeable and beginner

Recruiting process

- Individually defined, see SWC example
- Think about incentives, if you cannot find volunteers

www.iot-butler.eu

Key Messages

- **Consider the Customer Insight Interviews as a chance to get direct feedback from prospective customers which can be used as input for next iteration of POC**
  - They do not have to like our use cases, we want their honest opinion, not just accolades
  - Negative or neutral feedback is valuable and certainly not directed at you personally
- **Take care, the interviewees normally want to please you.**
  - So listen carefully to what they say and what they might really think
  - Compare them saying "one should" or "other people might" to "I really like that" or "I could really use that"
- **It is really, really difficult to not influence the interviewees**
  - Take care to word your questions and descriptions as neutral as possible
  - Sometimes it is better to say nothing at all
- **We want as many diverse opinions as possible, so move out of your comfort zone**
  - Do not interview "clones" of yourself, try to find really different people to interview
  - Use the target group and the persona descriptions as your recruiting guidelines
  - People are generally happy to give their opinion, so don't be afraid to approach them

www.iot-butler.eu

Approach - Focus Use Cases

smartHealth
G1 - Park bench
G2 - Video Appointment
G3 - Fitness
G4 - Allergies
G5 - Choice of Seat
smartHome
H1 - Kitchen
H2 - Fridge
H3 - Watering
H4 - Remote Control
H5 - Control from a Distance
smartEnergy
E1 - Washing Machine
E2 - Washing Machine Runs
E3 - Eco Monitor
E4 - Lights Control

User Story Picture has been presented for each Use Case to support the interviewee`s imagination :

G1: Park bench

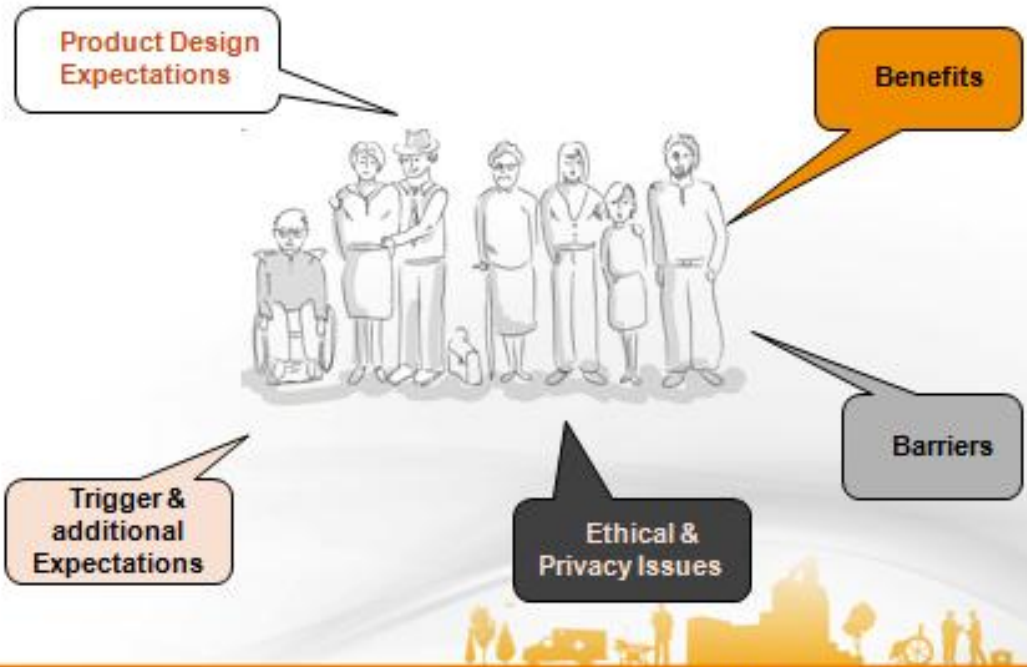
„During her walk…“

3 Main Topics have been selected:

- Health
- Home
- Energy

Approach (4) - Focus Topics

„How do you feel about this? “, looking at the …



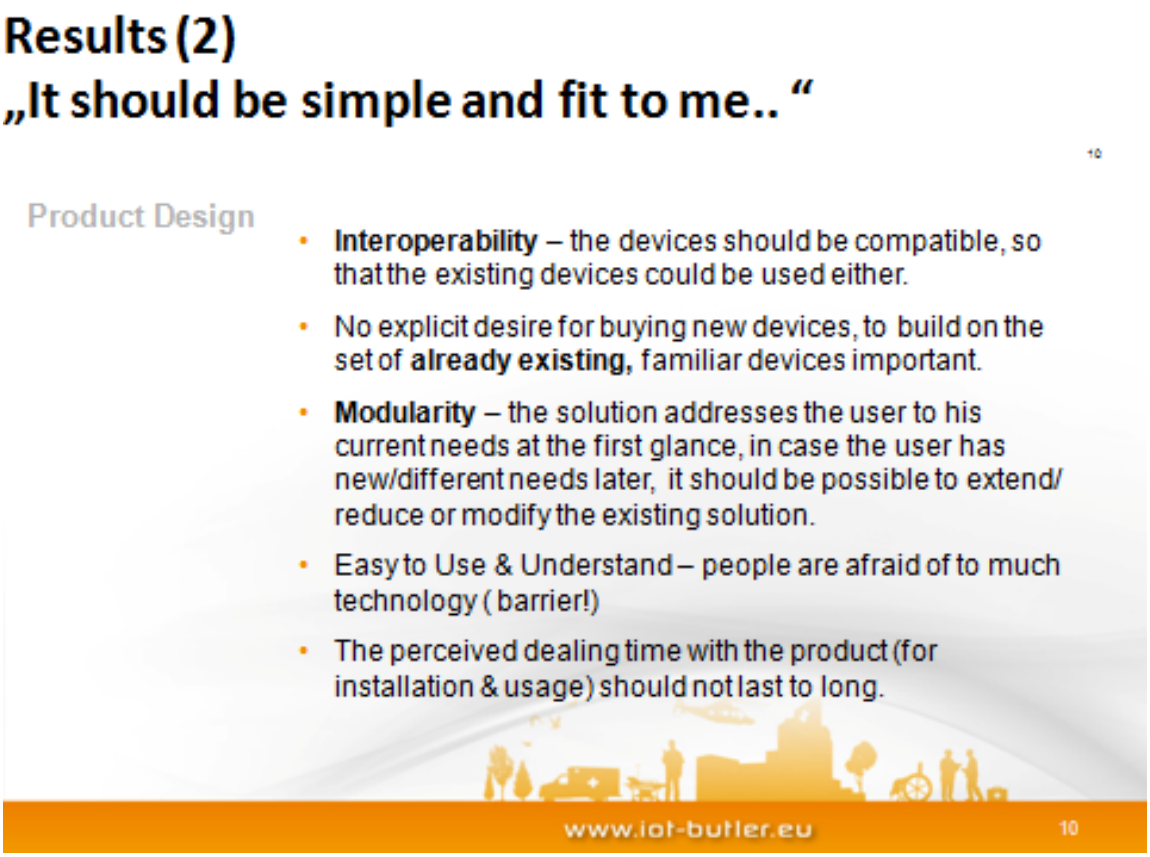
B.2 Sample material used for interviews

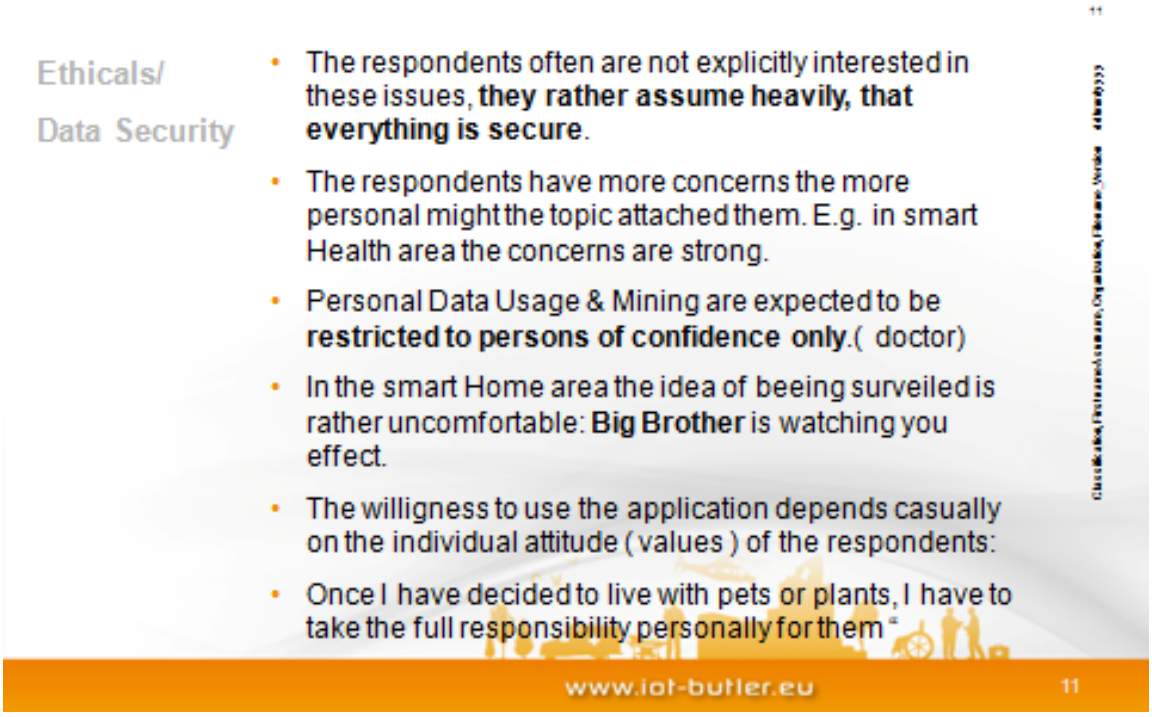
The interviews lasted around 1 hour each and the following material was used to support the process:

The interviewees were presented with images describing the use case, accompanied by a brief introduction of the use case by the interviewer:

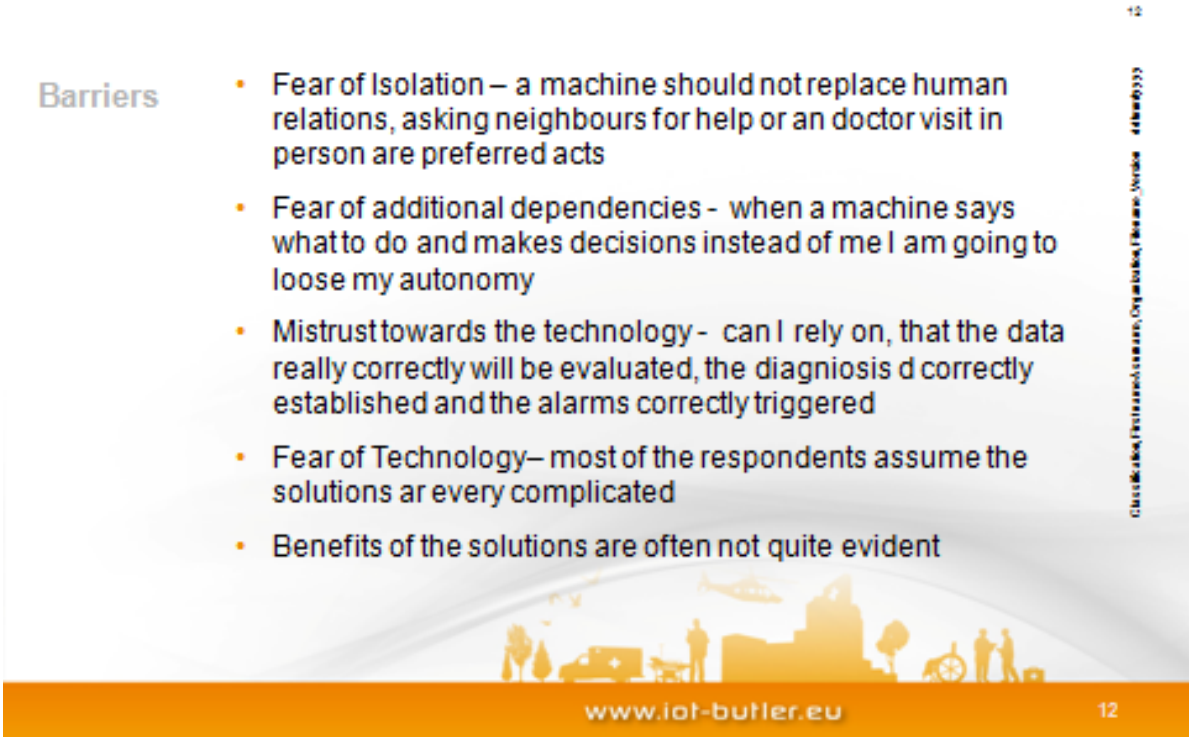
B.3 Results

The following are some initial results of the interviews; the complete results will be published and analyzed in BUTLER project deliverable 1.3: socio-economic impact.





Results (4)
„I don`t want to get rid of humans...“



Results (5)
„The benefits of the solution should be transparent and measurable “