Privacy & Us

D4.1 User Interface Requirements

Deliverable Number	**D4.1**
Work Package	WP 4
Version	1.00
Deliverable Lead Organisation	USE (USECON)
Dissemination Level	Public
Contractual Date of Delivery (release)	2017/05/31
Date of Delivery	2017/05/31
Status	**Final**

Editor

Michael Bechinie (USE)

Contributors

Patrick Murmann (ESR-1-KAU), Agnieszka Kitkowska (ESR-2-KAU), Poornigha Santhana Kumar (ESR-4-USE/UoS), Majid Hatamian (ESR-5-GUF), Alexandr Ralien (ESR-6-ULD), Juan Quintero (ESR-7-UNI/FAU), Lamya Abdullah (ESR-10-UNI/FAU), Alexandros Mittos (ESR-11-UCL), Mark Warner (ESR-12-UCL), Andreas Gutmann (ESR-13-VDS/UCL)

Reviewers

Eran Toch (TAU), Tom De Wasch (VDS)

This project has received funding from the European Union's Horizon 2020 research and innovation programme under the Marie Skłodowska-Curie grant agreement No 675730.

European Commission

Abstract

This deliverable summarises the identified high level user interface requirements from the specific ESR projects. These described requirements where gathered by the ESRs through different methods. This document will focus on types of requirements associated with the topic of “user interface”.

The preliminary considerations of each ESR already show that user interfaces play an important role in any type of product, system or service. Although all projects are in an early stage, taking high level user interface requirements already into consideration is of high value for the later stages. Many of the ESRs base their user interface requirements considerations on well-established heuristics, like defined by (Nielsen & Molich, NieMol90, 1990).

The user interface requirements for each ESR are based on the ISO/IEC/IEEE 29148:2011 standard (ISO, IEC, & IEE, 2011) and are documented in the same structure, containing a short description of the scope of each project, followed by a set of user interface requirements. The documented requirements reflect preliminary considerations, as all ESRs are in an early stage of their projects. In terms of the human centred design approach (International Organization for Standardization, 2010), leading to products, systems and services that are usable and having an adequate user experience the user interface requirements will change / evolve over time.

Table of Contents

1 Introduction

1.1 Purpose

This deliverable summarises the identified high level user interface requirements from the specific ESR projects. These described requirements where gathered by the ESRs through different methods. This document will focus on types of requirements associated with the topic of “user interface”.

This document will have dependencies to other deliverables within the same work-package (WP 4) and other work-packages (WP 2). Stakeholder and functional requirements shall be documented in D2.1 Requirements Analysis (Privacy&Us, 2017). Details of the user interface design and the concrete design of the system shall be documented in D4.2 User Interface Designs and Prototypes (Privayc&Us, 2017)

1.2 Writing requirements

The documentation of the specific requirements from the different ESR projects is based on the ISO/IEC/IEEE 29148:2011 standard (ISO, IEC, & IEE, 2011). This standard specifies:

- required processes for the engineering of requirements for systems and software products and services throughout their life cycle
- required information items and their required contents, and
- gives guidelines for the format of the information items

1.2.1 Construct

Requirements are statements that express needs and their associated constraints and conditions. They can be written in the form of a natural language. If expressed in that way, the statement should contain a subject, a verb and a may contain a complement. A requirement shall describe the subject of the requirement and what shall be done, and if additional criteria or conditions are needed.

> *Example 1: The coffee machine **[Subject]** shall clearly show if the power is off or on **[What]**, whether or not the electricity cable is plugged in or unplugged **[Condition]**.*
>
> *Example 2: **[Condition]** At power on state, the coffee machine **[Subject]** shall clearly show the on state **[What]**, with a green lamp **[Constraint]**.*

1.2.2 Language criteria

Requirements should describe 'what' is needed, not 'how' it will be realised. Requirements should not include concrete design solutions. However certain high level design decisions / solution architectures should be defined.

Of high importance is that each specified requirement shall have an indication about the level of obligation:

- “Shall” – Requirements that are mandatory binding necessities
- “Should” – Preferences or goals that are desired, non-binding necessities
- “May” – Suggestions that are non-mandatory, non-binding necessities

Undefined and general terms shall be avoided. They lead to requirements that are often difficult or even problematic to verify or leave room for various interpretations. The following are types of unbounded or ambiguous terms:

- Superlatives (e.g. 'best', 'most')
- Subjective language (e.g. 'user friendly', 'intuitive', 'cost effective')
- Vague pronouns (e.g. 'it', 'this', 'that')
- Ambiguous adverbs and adjectives (e.g. 'almost always', 'significant', 'minimal')
- Open-ended, non-verifiable terms (e.g. 'provide support', 'but not limited to', 'as a minimum')
- Comparative phrases (e.g. 'better than', 'higher quality')
- Loopholes (e.g. 'if possible', 'as appropriate', 'as applicable')

- Incomplete references (not specifying the reference with its date and version number; not specifying just the applicable parts of the reference to restrict verification work)
- Negative statements (like statements of system capability not to be provided)

1.2.3 Attributes

Well-formed requirements should have descriptive attributes defined to ensure the engineering process – understanding and managing the requirements.
This document shall focus on types of requirements associated with the topic of "user interface". Functional requirements shall be documented in [D2.1] Requirements Analysis.

- **Unique identifier.** Each requirement shall be uniquely identified (i.e., number, name tag)
- **Description.** Each requirement shall be clearly described. Specify how the system shall interact with external systems (external interface), or how system elements within the system, including human elements, interact with each other (internal interface). See **Error! Reference source not found. Error! Reference source not found.** how to describe the requirements.
- **Priority.** The priority of each requirement should be specified. As appropriate a simple scheme such as High, Medium, or Low, could be used.
- **Dependency to other requirements**. The dependency between requirements should be defined, if necessary.
- **Risk.** Analysis techniques may be used to determine a classification for system requirements in terms of their consequences. Major risks are connected to potential loss (financial, business opportunity, confidence by stakeholders), environmental impact, safety and health issues, and national standards or laws.
- **Source**. Each requirement should include an indication about the originator. Multiple sources may be considered.
- **Rationale**. The rationale behind each requirement should provide the reason that the requirement is necessary and points to any supporting evidence (e.g. analysis, study, modelling, or simulation). A potential source for general guidance are for example the usability heuristics (Nielsen, 1994).
- **Additional attributes.** One or more additional attributes may be assigned to each requirement.
    - Design Constraints – Define potential limitation to the design of the system by inflicting set boundaries and limits (e.g. legislation, standards and/or regulations).
    - Human Factors – Outline required characteristics for the outcomes of interaction with human users (and other stakeholders affected by use), e.g. in terms of safety, performance, effectiveness, efficiency, reliability, maintainability, health, well-being and satisfaction. These include characteristics such as measures of usability, including effectiveness, efficiency and satisfaction; human reliability; freedom from adverse health effects etc.

1.3 Format

The user interface requirements for each ESR are documented in the same structure.

1.3.1 Scope

This paragraph contains a short description of the scope / scenario / context of the specific ESR project.

1.3.2 User Interface Requirements

Each user interface requirement is documented separately.

UIREQ-ESR##-###-keyword	
Description	
Priority	
Dependency	
Risk	
Source	
Rationale	
Additional attributes	

Example

UIREQ-ESR099-005-showstate	
Description	The coffee machine shall clearly show if the power is off or on, whether or not the electricity cable is plugged in or unplugged.
Priority	[X] High, [ ] Medium, [ ] Low
Dependency	Depending from UIREQ-ESR099-004
Risk	If the user is not able to clearly see if the power is on or off the user can probably be exposed to a dangerous situation (electric shock) when plugging in the cable to a power outlet.
Source	Observation
Rationale	Visibility of system status: The system should always keep users informed about what is going on, through appropriate feedback within reasonable time.
Additional attributes	Mandatory accordingly ISO-12345

1.4 Acronyms / Abbreviations

Abbreviation	Meaning
A11Y	Accessibility – making a system accessible to groups of people with disabilities
GUF	JOHANN WOLFGANG GOETHE UNIVERSITAET FRANKFURT AM MAIN
GDPR	General Data Protection Regulation
HCI	Human Computer Interface
IoT	Internet of Things
KAU	KARLSTADS UNIVERSITET
L10N	Localization –translating the interface of a system to another language (numeronyms like this one refer to the number of letters between the first and the last one, and are widely accepted terminology in software engineering and interface design)
TAU	TEL AVIV UNIVERSITY
TET	Transparency enhancing technology/tool'
UC	UNIVERSITY COLLEGE LONDON
ULD	UNABHAENGIGES LANDESZENTRUM FUER DATENSCHUTZ
UNI	UNISCON UNIVERSAL IDENTITY CONTROL GMBH
USE	USECON THE USABILITY CONSULTANTS GMBH
VDS	VASCO
WU	WIRTSCHAFTSUNIVERSITAT WIEN

1.5 Terminology

Term	Explanation
Personal data	Refers to the term as specified in the GDPR.
Privacy	Refers to 'information privacy' or 'data privacy' as discussed by (van den Hoven, Blaauw, Pieters, & Warnier, 2016).
Transparency	The principle as stipulated in Chap. III, Art. 12 of the GDPR.
User	Refers to the user of a TET, which may be the data subject whose data is being reviewed or managed, or a legal representative or guardian.
Mode	A characteristic of an interface, where the same user-performed action can have different effects, depending on the current state of the system. An example of this is the Caps Lock key, which changes the state of the keyboard such a key will produce a capital letter; when Caps is off – the same key will type a small letter. (Raskin, 2011)
Quasi-mode	An alternative mode, that is active only when a particular action is carried out. For example, Shift + key will type a capital letter, but this mode is turned off as soon as shift is released. A person cannot forget that they are currently holding Shift pressed, while it is easy to forget that some minutes ago you pressed Caps Lock.
Mode error	An error that is caused by the fact that the user was unaware of the current mode of the system. This can produce harmless errors that are merely annoying – like typing a password with CapsLock, but it can also lead to major disasters – like disengaging autopilot on a plane, but thinking that it is still on auto (Chiles, 2008) (Casey, 1993)

2 User Interface Requirements

The following chapters summarize preliminary considerations of the ESRs in relation to their specific research projects. Each chapter has a short description of the scope of the specific project, followed by a set of user interface requirements. In terms of the human centred design approach (International Organization for Standardization, 2010), leading to products, systems and services that are usable and having an adequate user experience the user interface requirements will change / evolve over time. In relation to that approach the documented user interface requirements represent a “snapshot” of the current status of each project.

2.1 ESR-1 (KAU) Patrick Murmann - Usable transparency

2.1.1 Scope

This section specifies the user interface requirements (UI-requirements) of the ESR-project ‘Usable Transparency.’ The goal of this research project is to assess and classify the conceptual and technical requirements necessary to design usable transparency enhancing tools (TETs) in the context of data and information privacy.

2.1.2 User Interface Requirements

UIREQ-ESR01-001-AUDIENCE	
Description	The UI of the TET shall be designed for a specific target audience whose socio-cultural background, previous knowledge, and expectations have been comprehensively analysed during the requirement analysis phase of a software development life cycle. The UI shall be designed in such a way as to build upon that group's background and to work towards sufficing its respective expectations. The UI of the TET shall therefore take into account the particular conception of privacy of the intended target audience.
Priority	High
Dependency	None
Risk	The actual users of the TET might differ from the ones it was designed for, which might lead to unexpected behaviour on part of the users.
Source	(International Organization for Standardization, 2006) demands conformity with user expectations as a core principle of system dialogues. (ISO 9241-210: 2010, 2010) demands that the design of a system requires its context of use be clearly identified and specified as part of the development life cycle. It also demands that user and organisational requirements be specified before design solutions and actual prototypes be produced. (ISO/IEC/IEEE, 2011) second that.
Rationale	The TET shall be usable by the designated target audience. The principles of user-centred design suggest a software life cycle as stipulated in the aforementioned sources.
Additional attributes	None

UIREQ-ESR01-002-COMPREHENSIBILITY	
Description	The UI of the TET shall be designed in such a way that it is comprehensible and understandable by the intended user group. Comprehensibility refers to a user of the system being able to understand the visualisation of each operating step of the underlying process.

	The UI of the TET shall take into account the specific mental model, expertise, and domain knowledge of the targeted user group.
Priority	High
Dependency	UIREQ-ESR01-001-AUDIENCE
Risk	If the user of the TET is unable to understand the UI, he or she might be unable to use it in the way it was designed for. This discrepancy may lead to (1) decreased efficiency, (2) the user being effectively unable to use it at all, or (3) the user being unsatisfied with interacting with the TET.
Source	Nielsen et al. (Nielsen & Molich, NieMol90, 1990) stipulate that a usable system must "speak the user's language". The display of the system (Nielsen J. , Nielsen94, 1994) status shall be self-descriptive (International Organization for Standardization, 2006). The UI should be recognisable rather than recallable (Nielsen & Molich, NieMol90, 1990). Efficiency, effectiveness, and user satisfaction are specified in (International Organization for Standardization, 1998).
Rationale	In order to be comprehensible, the UI design shall take into account the specific previous knowledge of the target group when using termini, semiotics, and visualisations.
Additional attributes	None

UIREQ-ESR01-003-FEEDBACK	
Description	The UI of the TET shall provide noticeable feedback to all actions triggered by the user. It shall likewise provide meaningful feedback, if the system state changes due to asynchronously or externally triggered events. In the event of a change of state, the TET shall provide information sufficient to complete the user's task effectively. It must be clear which implications a change of state has for the user's privacy.
Priority	High
Dependency	UIREQ-ESR01-002-COMPREHENSIBILITY
Risk	A lack of feedback in terms of incorrectly reflecting the system status and the actual implications for the user's privacy might lead to misconfiguration or an unintended use of the TET. Both might have an unanticipated impact on the user's privacy.
Source	(Nielsen J. , Nielsen94, 1994) lists the "visibility of system status" and a "match between system and the real world" as principles for the UI-design. (Schlegel, Kapadia, & Lee, 2011) states that "applications without an appropriate means of exposure feedback and control can lead to unintended privacy breaches."
Rationale	The system shall always keep users informed about what is going on, regardless of the cause that led to the change of status. If the status of the TET changes without the user being informed accordingly, the user (1) might assume a state that differs from the actual system state, (2) might be confused while interacting with the system at a later stage, and (3) might be unsatisfied with the course of future events while interacting with the TET due to being unable to anticipate the behaviour of the TET.
Additional attributes	None

UIREQ-ESR01-004-CONTROLABILITY	
Description	The UI of the TET shall permit users to exercise control during each individual step of the operating process. If the UI visualises a transactional process that consists of multiple operating steps, the UI shall enable users to cancel the entire process at any time until the final operation step of the transaction is confirmed.
Priority	High
Dependency	UIREQ-ESR01-003-FEEDBACK
Risk	The lack or loss of control might lead to an unintended use of a TET, which might have an unanticipated impact on the user's privacy. If the user of the TET is unable to exercise control, the underlying process might not be completed effectively, efficiently, or satisfyingly.
Source	(International Organization for Standardization, 2006) stipulates controllability as a core principle of system dialogues. (Nielsen J. , Nielsen94, 1994) demands "user control and freedom" as a core principle of UIs. The studies conducted by (Balebako, Jung, Lu, Cranor, & Nguyen, 2013) and (Fischer-Hübner, Angulo, Karegar, & Pulls, 2016) conclude that users appreciate being in control of their personal data. (Hsieh, Tang, Low, & Hong, 2007) and (Kani-Zabihi & Helmhout, 2012) stipulate control over one's personal data as a central requirement for the design of their respective TET.
Rationale	Once the user has started a task using the TET, he or she shall be in control of the process at any given time until the task is finished.
Additional attributes	The UI shall allow users to approve or to disapprove each operating step. If the TET allows for parameterising multiple settings as part of the same operating step, approving and disapproving each of them shall be possible in a clearly transparent way.

UIREQ-ESR01-005-CUSTOMISATION	
Description	The UI of the TET shall allow users to customise their privacy settings according to their personal needs, as well as to organisational or legal constraints, respectively. It shall allow users to specify and audit the conditions under which specific kinds of personal data are disclosed to specific data controllers and downstream processors.
Priority	High
Dependency	UIREQ-ESR01-004-CONTROLABILITY
Risk	A TET that cannot be customised according to the needs of an individual user might prevent that user from effectively using the TET. If the configuration of the TET does not reflect the user's actual needs, the control of his or her personal data might be incomplete or incorrect. A lack of customisation on part of the TET might result in it being usable only in an inefficient or non-satisfactory way.
Source	Individualisation aids users in accomplishing their task more efficiently or more satisfyingly (International Organization for Standardization, 1998). (International Organization for Standardization, 2006) and (International Organization for Standardization, 2010) stipulate suitability for individualisation as a core principle of system dialogues.
Rationale	The UI shall allow users to customise individual privacy preferences. The TETs discussed in scientific literature are demarcated exactly by the kind

	and extend of customisation they allow users in terms of expressing their privacy preferences in the respective usage context.
Additional attributes	(International Organization for Standardization, 2006) and (International Organization for Standardization, 2010) stipulate the suitability for the underlying task as a core principle of system dialogues. Consequently, an excessive customisability of a TET might reduce its effectiveness or efficiency for the task it was originally intended for.

UIREQ-ESR01-006-GRANULARITY	
Description	Users of the TET should be able to switch between multiple levels of details when the TET provides them with either a large amount of data items, or with data items that consist of many subordinate components or elements. Varying granularity might be required due to a user's personal preferences or previous knowledge. It might also be stipulated by regulatory authorities, such as organisational bodies or the law.
Priority	Medium
Dependency	UIREQ-ESR01-002-COMPREHENSIBILITY, UIREQ-ESR01-005-CUSTOMISATION
Risk	Non-adaptable granularity might lead to information being displayed as either coarse-grained or fine-grained. Either level of detail might be suboptimal for particular usage contexts or for the personal needs of particular users. In such cases, using the system might be inefficient or non-satisfactory.
Source	(Nielsen J. , Nielsen94, 1994) lists "Flexibility and efficiency of use" as one of the usability heuristics of UIs. In the context of PETs, Reeder et al. (Reeder, Kelley, McDonald, & Cranor, 2008) study extensible UIs that are adaptable to the user's personal taste and requirements, and state that they satisfy the demand for multiple levels of detail.
Rationale	Different users have different requirements as regards the perspective used to monitor and control personal data.
Additional attributes	None

UIREQ-ESR01-007-ADAPTABILITY	
Description	The UI of the TET should take into account choices users have made in the past, and reflect previous choices when offering respective options in the present. The UI of the TET may reintroduce or prioritise contextual decisions based on previous choices of the users once they modify their privacy preferences at a later time.
Priority	Medium
Dependency	UIREQ-ESR01-005-CUSTOMISATION
Risk	Users might find the default settings inappropriate for or non-applicable to their personal needs. A lack of individualisation might result in inefficient or non-satisfactory use of the TET.
Source	Individualisation aids users in accomplishing their task more efficiently or satisfyingly (International Organization for Standardization, 1998).
Rationale	The user's mental model should be reflected in the interaction with the TET. Being confronted with an UI that does not sufficiently reflect the user’s mental model, he or she might be alienated, and complete the designated task less efficiently or satisfyingly.
Additional attributes	None

UIREQ-ESR01-008-PROXYING	
Description	Individual operating steps of a transactional process that serves the purpose of requesting decisions from a user may be skipped, if doing so results in the underlying process being completed more efficiently or more satisfyingly for the user. In this case, the TET acts as a proxy for the user, and makes respective choices regarding the user's privacy in his or her stead. For example, a TET may automatically decide on behalf of its user whether queries related to individual personal data items of the data subject are acceptable. In order to satisfy the user's interests, decisions made by a proxy shall be inferred from choices he or she made in the past, or from preferences specified. Automated decisions shall be auditable by the user at a later time.
Priority	Low
Dependency	UIREQ-ESR01-005-CUSTOMISATION , UIREQ-ESR01-007-ADAPTABILITY
Risk	Users might find it tedious to respond to large amounts of queries of their personal data. This might result in inefficient or non-satisfactory use of the TET on the long run.
Source	(International Organization for Standardization, 1998) defines the terms efficiency and satisfaction. (Sadeh, et al., 2009) and (Kelley, Hankes Drielsma, Sadeh, & Cranor, 2008) argue that users that share personal data in the context of location-based services appreciate machine-based decision making on their behalf, and that respective predictions can be made with high accuracy, respectively.
Rationale	Machine-based decision making may support users in making decisions more efficiently or more satisfyingly.
Additional attributes	None

2.2 ESR-2 (KAU) Agnieszka Kitkowska - Measuring and manipulating privacy related attitudes and behaviors

2.2.1 Scope

This document extracts the User Interface (UI) requirements for the project 'Measuring and manipulating privacy related attitudes and behaviours'. The project's overall goal is to develop interface elements that influence decision-making process, leading to the increased privacy awareness and to the informed decisions considering harms, and resulting risks.
The specified requirements are concentrated on the Graphical User Interface (GUI). However, some of the functional requirements are inherent to GUI.

2.2.2 User Interface Requirements

UIREQ-ESR02-001-VISIBILITY	
Description	The UI must be designed in a way that privacy relevant information and alerts are easily accessible and visible at all time. However, the information and alerts must be displayed in a way that does not disturb the user and do not add to the cognitive workload. The information

	visibility should be initiated by the user unless there are significant risks to privacy violations, than the system should display notification without user's action. This calls for a balance between the user's control and disturbing nature of alerts.
Priority	High
Dependency	
Risk	If the user is not able to access information in easy and timely manner, it may influence risky behaviour. If the user experiences real-time feedback too often or within irrelevant situations, it may cause a cognitive overwork, loss of interest, frustration, and even panic. In a result, there may be a risk of negative psychological impact and loss of confidence. If the user is unable to locate privacy relevant information, including help and documentation, the risk of legal incompliance increases (accordingly to GDPR Art. 12 (EU, 2016)). This may result in economic losses.
Source	Observation, experience and literature.
Rationale	• The usability principle *visibility of the system status*; *access to help and documentation*; *aesthetic and minimalistic design* (dialogues should not contain irrelevant or rarely needed information) (Nielsen, 1994) • The user experience principle of *self-descriptiveness.* The users are always aware of their current place in the dialogue, which actions they can perform and how to proceed with them (International Standardization Organization (ISO), 2009) • The role of visibility and users mental over workload emphasised by Fischer-Hubner et al.: *System designers should try to minimize the users' memory load by increasing the visibility of interactive elements, accommodating affordances, and supporting intuitive interactions* (Fischer-Hübner, Angulo, Graf, Wastlund, & Wolkerstorfer, 2011).
Additional attributes	There is a risk that information displayed too often may build a habit of ignorance or disturbance.

UIREQ-ESR02-002-CONSISTENCY	
Description	The UI should be consistent, both at visual and functional level, independently of technology. The UI elements must be familiar to the user, and designed accordingly to the globally recognized patterns and guidelines.
Priority	High
Dependency	
Risk	The inconsistent design of the UI may result in cognitive overwork and uncertainty. This may trigger feelings of frustration, panic and develop dissatisfaction. If the UI is inconsistent with standard design approaches and guidelines defined by research and industry, there is a risk that user will not understand how to interact with the interface. This causes social exclusion. The inconsistency and incompatibility of the UI design with different platforms may result in economic exclusion (users who cannot afford certain technology cannot use the system) and stakeholder's financial loss (system available only to a limited number of users).

Source	Observation, experience, literature and industry examples.
Rationale	• Requirement for *consistency and standards* implies that users should not have to wonder whether different words, situations, or actions mean the same thing (Nielsen, 1994). • It is necessary to create consistent designs that influence people's *affordances* – users have expectations regarding the system layout, and if these expectations are not met users' need to *learn twice* (pp. 92, Benyon, 2010).
Additional attributes	As per Benyon, consistency is a slippery concept. Sometimes, it is required to implement inconsistent design elements that draw users' attention to something important, and in result it may change user's decisions. This is important in the context of privacy, where the design should impact users' decisions and therefore, inconsistencies may be beneficial to the harms and risks communication.

UIREQ-ESR02-003-ACCESSIBILITY	
Description	The information shall be provided in comprehensive and universally acceptable form, and it must be compliant with accessibility standards such as W3C accessibility guidelines, ISO/IEC 40500:2012 and EN 301 549 v1.1.2.
Priority	High
Dependency	UIREQ-ESR02-001-VISIBILITY
Risk	If the code underlying the UI is not compatible with accessible technologies, such as screen readers there is a risk of physical exclusion. If the commands are obscure and information presented in a complicated manner, users' may not be able to construct mental models of the system. This may result in the conceptual exclusion. If UI is inaccessible throughout all types of technology, it may result in economic and social exclusion, as well as stakeholders' financial losses.
Source	Observation and research literature.
Rationale	• British Accessibility Standard BS8878. • World Wide Web Consortium (W3C accessibility guidelines). • ISO/IEC 40500:2012. • EN 301 549 v1.1.2. • Design must be accessible for all to avoid exclusion of people from different age groups, people with disabilities etc. (*inclusive design*) (pp.80, Benyon, 2010).
Additional attributes	

UIREQ-ESR02-004-CONTROL	
Description	The UI shall ensure and enhance control over the privacy related decisions by providing an appropriate information and feedback. The UI must provide information about the possible harms and benefits related to privacy decisions, such as feedback about the data collection, processing and dissemination.
Priority	High
Dependency	

Risk	If the user is unaware of what information is being captured, and why and how they can access it, the risk of uninformed privacy decisions increases. If the user is not provided with an appropriate feedback, whether it is a visual cue or interaction method, there is a risk of loss of control over data and violation of legal compliance (GDPR). If the user is provided with too much of control, it may lead to the *control paradox* and result in information over-exposure.
Source	Academic publications, industry guidelines.
Rationale	• The usability requirement defined as *control and freedom* (Nielsen, 1994). Users often choose system functions by mistake and will need a clearly marked "emergency exit" to leave the unwanted state without having to go through an extended dialogue. Support undo and redo. • The ISO9241-210 lists *controllability* as one of the principles for user experience design (International Standardization Organization (ISO), 2009). • Research demonstrated the existence of the *control paradox:* when people's perceived control over personal information increases, they willingness to the data exposure also increases (Brandimarte, Acquisti, & Loewenstein, 2013). • Necessity to provide a greater control to users who want to share information, but should be able to control the circumstances under which the information is shared (Benisch, Kelley, Sadeh, & Cranor, 2011).
Additional attributes	

UIREQ-ESR02-005-LEARNABLITY	
Description	The UI functionality and design shall be easy to learn and understand. The interface should consists of elements familiar to the users, simple, representing real world and enabling representative mental models. Therefore, the recognition based designs should be implemented, relating to the real life examples.
Priority	High
Dependency	UIREQ-ESR02-001-VISIBILITY; UIREQ-ESR02-002-CONSISTENCY
Risk	If user do not recognize design elements, the risk of un-protective behaviours increases. The UI difficult to understand and learn may lead to risk of social or cultural exclusion. If there is a lack of understanding of UI, the time of task performance increases. This may result in a risk of stakeholder economic loss (decreasing numbers of users).
Source	Observation and literature.
Rationale	• The ISO9241:210 defines the *suitability for learning* as one of the principles for user experience design (International Standardization Organization (ISO), 2009). • The *learnability* is listed as one of the principles supporting usability: *the ease with which new users can begin effective interaction and achieve maximal performance* (pp. 260, Dix, Finlay, Abowd, & Beale, 2004).

Additional attributes	The learnability aspects are problematic because users are often goal-oriented and are not willing to learn. The time and context shall be considered as additional constrains to learnability.

UIREQ-ESR02-006-DEFAULTS	
Description	The UI should clearly present 'defaults' that are appropriate to the user expectations not to the designers' ideas. The defaults should align with users' needs defined by individual privacy expectations. They shall be visible and easily accessible at any point of interaction. The defaults must be in line with the GDPR.
Priority	Medium
Dependency	
Risk	If the defaults are inappropriate, there is a risk of users' false assumptions about how the UI works. Therefore, the risk of psychological exclusion increases. If user is unable to change the default settings, there is a risk of decreased satisfaction and increased frustration. This may lead to stakeholders' losses, such as financial and reputation. If the default settings opt-out and opt-in are not clearly visible, the users may never amend the original settings, presuming their implicit recommendation.
Source	Observation and literature.
Rationale	• ISO9241:210: *suitability for individualization* (International Standardization Organization (ISO), 2009). • As per previous research, the way that the defaults are presented to the users is frequently responsible for people's choices (framing effect) (Johnson, Bellman, & Lohse, 2002). • The inappropriately presented defaults may lead to the blind belief that settings should not be changed (Acquisti, Brandimarte, & Loewenstein, 2015; Schaub, Balebako, Durity, & Cranor, 2015).
Additional attributes	

UIREQ-ESR02-007-EFFIENCY	
Description	The UI must include interaction techniques that retain users engaged and informed at all time, decreasing boredom and preventing loss of interest. Simultaneously, the UI shall not include irrelevant information or unnecessary interaction methods.
Priority	Medium
Dependency	UIREQ-ESR02-002-CONSISTENCY; UIREQ-ESR02-005-LEARNABLITY; UIREQ-ESR02-006-DEFAULTS
Risk	If user is not engaged in interaction, there is a risk of low interest in the displayed information. This may result in stakeholder economic losses. If the interface does not include interaction methods and visually pleasing, aesthetic designs, users' expectations of the system may not be met.
Source	Observation, literature and industry news.

Rationale	• Accordingly to Nielsen the *aesthetic and minimalist design* is one of the usability heuristics (Nielsen, 1994). It claims that dialogues should not contain information which is irrelevant or rarely needed and every extra unit of information diminishes visibility. • The *representational design* should be implemented. As per Benyon, *representational design* is *concerned with fixing colours, shapes, sizes and information layout. It is especially important for issues such as the attitudes and feelings of people, but also for the efficient retrieval of information* (pp. 54, Benyon, 2010).
Additional attributes	

UIREQ-ESR02-008-VISUAL CUES	
Description	The UI shall contain easily understandable visual alerts about the risks associated with the system usage. The use of icons or other images is advisable, however, the more complex concepts of risks should be accompanied with text descriptions. The alerts must be presented at an early use-stage and subtly repeated throughout the rest of the user's interaction.
Priority	Medium
Dependency	UIREQ-ESR02-001-VISIBILITY; UIREQ-ESR02-002-CONSISTENCY
Risk	If the user is not provided with persuasively presented risk information, it may lead to an increased exposure and harms. This could result in social exclusion and distortions. If the design does not include appropriate visual cues (icons), the stakeholders are exposed to economic loss due to the lack of legal compliance (GDPR).
Source	Observation and research literature.
Rationale	• The usability heuristics such as *visibility of the system status* (user always informed about what is happening via properly designed fe within reasonable time) and *recognition rather than recall* (Nielsen, 1994). • The icons should be used to communicate privacy information, however, they have to be *personalized* and *contextualized* (ENISA, 2013). • The alerts should be designed in such a manner, that clearly present whether the risk *can be* or *should not be* ignored (pp. 334, Benyon, 2010). • The textual privacy notices should be free of language ambiguities (Schaub et al., 2015; Bruening & Culnan, 2015).
Additional attributes	There is a risk of overwhelming user with risks alerts that are too visible, decreasing efficiency of the task-achievement. Similarly, this may lead to skewed behaviours, such as overprotection or under-protection.

UIREQ-ESR02-009-CONSENT	
Description	The consent should contain visual cues and simple language. The visual cue should consists of icons or other elements recognizable by the diverse users. The visual cues should be representative of real-life forms and symbols to increase recognition.
Priority	Medium

Dependency	UIREQ-ESR02-001-VISIBILITY; UIREQ-ESR02-002-CONSISTENCY; UIREQ-ESR02-008-VISUAL CUES
Risk	If the consent is difficult to understand users may over-disclose their information. Therefore, their identity becomes exposed to harms, such as distortion, identification, unintended use of the information and more. Considering demographic diversity of users the consent must present information in a universal form, to increase accessibility and ensure that the technology can be used globally. Otherwise, there is a risk of economic, social and cultural exclusion, as well as stakeholder financial loss.
Source	Observation and research literature.
Rationale	• The usability heuristic *match between system and the real world* (Nielsen, 1994). User interface should contain words, sentences and concepts familiar to the user. • The policies' display should be easy to locate and read, ensuring trust in the system (Shneiderman, 2000).
Additional attributes	

2.3 ESR-4 (USE/UoS) Poornigha Santhana Kumar - Designing for Privacy & Security at Point of Sale Commercial Transactions

2.3.1 Scope

My PhD thesis aims to deliver a secured and privacy enhanced experience for users at point of sale commercial transactions. We aim to provide user with control over their data and also prevent any attacks (theft of information) on their data. We focus on Near Field Communication (NFC) payments as it is commonly used in retail shops now-a-days. We also choose to work on retail shop checkouts as it involves wide range of customers (age, gender and profession) and accepts all types of payment (cash, credit/debit card, NFC in cards and mobile phones). We will be developing various transaction prototypes and evaluate them with potential users. The prototypes will be developed based on the following high requirements.

2.3.2 User Interface Requirements

UIREQ-ESR04-001-Card Display	
Description	Display only the information necessary for the transaction
Priority	Medium
Dependency	
Risk	The users feel insecure to reveal more information as their account can be easily compromised in case of theft
Source	Observation and Interviews with customers at retail shops
Rationale	Heuristics Principle: Minimalist design
Additional attributes	Bank principles

UIREQ-ESR04-002-Terminal UI	
Description	The place where the card/mobile has to be scanned should be marked clearly in the payment terminal
Priority	High
Dependency	Design of the payment terminal installed in that particular retail shops
Risk	If the place to scan NFC card or mobile is not marked clearly then the user cannot start the transaction

Source	Observing customer at retail shops
Rationale	The users are not aware of how to initiate the connection (transaction) between the NFC card/mobile and the payment terminal (Geven, 2007)
Additional attributes	

UIREQ-ESR04-003- Terminal UI	
Description	The amount to be paid should be displayed before paying
Priority	Medium
Dependency	
Risk	The user may doubt the amount being transferred if the amount to be paid is not explicitly displayed by the terminal
Source	Interviews with customers at retail shops
Rationale	Heuristics Principle: Error prevention
Additional attributes	Design of the payment terminal installed in that particular retail shops

UIREQ-ESR04-004- Terminal UI	
Description	The amount to be paid should be displayed in appropriate currency
Priority	Low
Dependency	
Risk	The user may doubt the amount being transferred if the amount to be paid is displayed in different currency by the terminal
Source	Interviews with customers at retail shops
Rationale	Heuristics Principle: Error prevention
Additional attributes	Design of the payment terminal installed in that particular retail shops

UIREQ-ESR04-005- Terminal UI	
Description	The state of the transaction should be displayed by the payment terminal
Priority	High
Dependency	
Risk	If the current state of the transaction is not displayed then the user may withdraw the card/mobile before the transaction ends
Source	Interviews with customers at retail shops
Rationale	Heuristics Principle: Visibility of system status
Additional attributes	Design of the payment terminal installed

UIREQ-ESR04-006- Terminal UI	
Description	Visual and audio feedback should be provided after the transaction
Priority	High
Dependency	
Risk	Both visual and audio feedback should be given so that all users (including the physically challenged users) knows that the transaction is complete
Source	Observation and Interviews with customers at retail shops
Rationale	NFC system should deliver multiple feedback such that it is noticed by all user (including the physically challenged users) (Tomitsch, 2008)
Additional attributes	Design of the payment terminal installed

UIREQ-ESR04-007-Application UI	
Description	Visual or sound indication to show the user that the mobile is ready to be scanned
Priority	High
Dependency	
Risk	The application should be ready when the user scans the mobile in the terminal. If not, the transaction will not be initiated
Source	Interviews with customers at retail shops
Rationale	Heuristics Principle: Visibility of system status
Additional attributes	The indication depends on the mobile model used and the mobile setting of the user

UIREQ-ESR04-008- Application UI	
Description	Display only the information necessary for the transaction
Priority	Medium
Dependency	
Risk	The users feel insecure to reveal more information as their account can be easily compromised in case of theft
Source	Observation and Interviews with customers at retail shops
Rationale	Heuristics Principle: Minimalist design
Additional attributes	Depends on the mobile model used

UIREQ-ESR04-009- Application UI	
Description	The state of the transaction should be displayed by the payment terminal
Priority	High
Dependency	
Risk	If the current state of the transaction is not displayed then the user may withdraw the mobile before the transaction ends
Source	Interviews with customers at retail shops
Rationale	Heuristics Principle: Visibility of system status
Additional attributes	Depends on the mobile model used

UIREQ-ESR04-010- Application UI	
Description	Based on user preference, visual or audio feedback should be provided after the transaction
Priority	High
Dependency	
Risk	visual or audio feedback (based on user preference) should be given so that all users (including the physically challenged users) knows that the transaction is complete
Source	Observation and Interviews with customers at retail shops
Rationale	NFC system should deliver multiple feedback such that it is noticed by all user (including the physically challenged users) (Tomitsch, 2008)
Additional attributes	Depends on the mobile model and the mobile settings used by the user

UIREQ-ESR04-011- Application UI	
Description	Display recent transactions when the user is authenticated
Priority	Medium

Dependency	
Risk	If the transaction list is not accessible the user may not be able to review their transactions when needed
Source	Interviews with customers at retail shops
Rationale	Heuristics Principle: User control and freedom
Additional attributes	Depends on the mobile model

UIREQ-ESR04-012- Application UI	
Description	Display options to block the card when the user is authenticated
Priority	Medium
Dependency	
Risk	The user should be able to block the card immediately in case of theft. If not, the card may be misused
Source	Interviews with customers at retail shops and literature study
Rationale	Heuristics Principle: Help users recognize, diagnose, and recover from errors
Additional attributes	Depends on the mobile model

UIREQ-ESR04-013- Application UI	
Description	Display options to change the authentication credentials of the application
Priority	Low
Dependency	
Risk	The user may feel insecure about their data if there is no possibility to change the password
Source	Interviews with customers at retail shops
Rationale	Heuristics Principle: User control and freedom
Additional attributes	Depends on the mobile model

2.4 ESR-5 (GUF) Majid Hatamian - Privacy Indicators in Smartphone Ecosystems

2.4.1 Scope

This document provides the user interface (UI) requirements necessary in smartphone ecosystems. The document is intended as a reference to introduce and highlight the foundational steps that must be taken into consideration for designing a usable UI. Therefore, several steps are discussed in order to analyse the needs essential for a usable application in smartphone ecosystems. Additionally, the importance of studying usability from two different perspectives including technical and psychological perspectives are introduced as a basis while developing and designing UI.

2.4.2 User Interface Requirements

UIREQ-ESR05-001 - User centric	
Description	The home screen should support sufficient information regarding the overall instructions for using different screens of the proposed prototype.
Priority	High
Dependency	---
Risk	The user will become disappointed of working with the prototype

Source	(Galitz, 2002)
Rationale	The user interface shall allow the user to focus on tasks and information provided regarding her privacy. In other words, we shall use an easy to learn user interface which enables users to interact with different menus, screens and components of artefact.
Additional attribute	Human Factor

UIREQ-ESR05-002 - Response time	
Description	The response time shall be less than 5 seconds. In our case, the response time is defined as the time that it takes for the user to send/receive any reaction from the user interface.
Priority	High
Dependency	UIREQ-ESR5-003, UIREQ-ESR5-007
Risk	The user will become disappointed of working with the prototype
Source	(Android, 2017)
Rationale	Waiting for a long tim to send/receive any reaction to/from the user interface leads to annoyance, tedium and it ultimately reduces system's performance (Galitz, 2002).
Additional attribute	Human Factor

UIREQ-ESR05-003 - Tedium	
Description	The proposed user interface should not be tedious. The interaction between user and user interface shall be kept in the maximum possible level of attractiveness. One potential solution is to provide users with informative privacy indicators. Users do not like to see non-informative privacy indicators with too many legal and technical descriptions.
Priority	High
Dependency	UIREQ-ESR5-002, UIREQ-ESR5-006, UIREQ-ESR5-007
Risk	The proposed prototype will become boring for the user
Source	(Johnson J. , 2010)
Rationale	Tedium happens when the user is not able to quickly and properly interact with app (e.g. long response times). Thus, it is essential to overcome this issue, othersie, it leads to frustration.
Additional attribute	Human Factors

UIREQ-ESR05-004 - Ambiguity	
Description	The user interface should be straightforward and not confusing for the user. The menus should be easy to reach and they should not be nested. Appropriate compbination of colours should be used to give the ability to the user to quickly identify different screens of the app.
Priority	High
Dependency	UIREQ-ESR5-006
Risk	The proposed prototype will become boring for the user
Source	(Johnson J. , 2010)

Rationale	The different components of app should be clear and understandable to every user with different kinds of knowledge, age, education, etc.
Additional attribute	Human Factors

UIREQ-ESR5-005 - Attractiveness	
Description	The app should be attractive. People do not want to follow what they do not like. Also, privacy indicators should concentrate the users' attention and they should not overwhelm users with meaningless indications. When it comes to designing privacy indicators for smartphone apps, the indicators should have different level of sensitivity. One possible way is to use distinguishable colours, e.g. red for dangerous accesses to permissions. Furthermore, using attentive icons is helpful, e.g. attention icon with yellow colour when an anomaly is recognised.
Priority	High
Dependency	UIREQ-ESR5-003
Risk	The proposed prototype will become boring for the user
Source	(Johnson J. , 2010)
Rationale	If the user interface will not be attractive for the user, this situation leads to tedium and ambiguity. Moreover, keeping the user interface attractive will influence the decisions that the users will take regarding their privacy (after receving the privacy indicators).
Additional attribute	Human Factors

UIREQ-ESR05-006 - Annoyance	
Description	User interface should not limit users' freedom. Importantly, privacy indicators should not annoy users with inappropriate information which prevents a normal task being completed. One potential solution is to design an efficient setting which allows user to optionally personalise everything according to their needs, e.g. the scanning time period, log intervals, scans storing time, etc. In addition, users should not force to receive/see any notification, e.g. using sticky notifications in the toolbar (action bar).
Priority	High
Dependency	UIREQ-ESR5-003
Risk	The proposed prototype will become boring for the user
Source	(Johnson J. , 2010)
Rationale	Difficulties in quickly finding information, out-dated information, and visual screen distractions are factors that may annoy users.
Additional attribute	Human Factors

UIREQ-ESR05-007 - Fear	
Description	User interface shall not impose fear on the user. The user interface shall be designed in such a way that user can rely on it, e.g. the log analysis and scans shall be stored safely in users' devices, and the users shall be able to retrieve them when they want. Importantly, privacy indicators shall not scare users with inappropriate way of representation, e.g. when the results of scans show some anomalies from some installed apps,

	this shall not be introduced to the user in a shocking way (with too vague or too direct terms)
Priority	High
Dependency	---
Risk	The user will not become motivated and attracted to work with the proposed prototype.
Source	(Johnson J. , 2010)
Rationale	Unavailability of app or some of its components which affect the users' normal routines may impose fear. Importantly, when user confronts with inappropriate privacy indicator which targets her sensitive personal data.
Additional attribute	Human Factors

2.5 ESR-6 (ULD) Alexandr Ralien - Usable Privacy in the Internet of Things and Smart Spaces

2.5.1 Scope

Smart Spaces – The requirements apply to public smart spaces that are not marked by strict borders and are accessible to anyone – e.g. city squares, parks, malls or bus stations. It is expected that the space will have tens or hundreds of people walking in and out of it in the course of an hour. IoT Devices – The requirements apply to personal IoT devices installed in households or carried by their owners. The devices may or may not have human-computer interface of their own. If an interface is not available, it is expected that people can interact with it through their smartphones, tablets or computers. Industry-grade IoT hardware, as well as IoT infrastructure installed in public spaces is not in scope.

2.5.2 User Interface Requirements Smart Spaces

UIREQ-ESR06-SP001-SIGNAL	
Description	The smart space shall signalize the people who walk into and out of it (e.g. like traffic signs or navigation hints in airports) (Raskin, 2011)
Priority	High
Dependency	
Risk	• If a person is unaware of the fact that they are entering a smart space, they cannot adjust their behaviour accordingly, which potentially leads to violations of privacy expectations or regulations (e.g. not seeing a “Stop” sign and thus ignoring it). • If a person depends on the smart space to sustain a state, they should know when they cannot depend on it anymore and adjust accordingly (e.g. relying on artificial gravity, then suddenly falling down like Wile E. Coyote)
Source	Literature, regulations
Rationale	• A smart space adds a *mode* to the environment, thus mode errors are bound to happen (Raskin, 2011) • GDPR Art. 13 – if personal data collection is taking place, people must be informed of it (in certain cases their consent is required too) and made aware of what is collected, for what purpose, for how long, etc (EC, n.d.).
Additional attributes	

UIREQ-ESR06-SP002-FLAVOUR	
Description	Each space should convey its capabilities (“smart space flavour”) in a standardized way (e.g. pictograms, Braille patterns).
Priority	High
Dependency	UIREQ-ESR06-SP001-SIGNAL
Risk	A person not knowing or understanding what makes a space “smart” cannot make a reasonable choice for their further actions. For example, if a person wants to conceal the fact that they are single, they will want to avoid walking into a space that renders a nimbus above the heads of single people.
Source	
Rationale	Smart spaces are “smart” in different ways, people cannot be expected to guess what they are walking into. • GDPR Art. 13 – specify for what purposes personal data are collected (EC, n.d.) • General usability requirement (Schaub, Balebako, Durity, & Cranor, 2015)
Additional attributes	

UIREQ-ESR06-SP003-CULTURE	
Description	The “smart space” signal should appeal to a cross-cultural audience.
Priority	High
Dependency	UIREQ-ESR06-SP006-CONSENT, UIREQ-ESR06-SP001-SIGNAL
Risk	Same as in SP002-FLAVOUR, but dealing with the fact that people who walk into the space can have different cultural backgrounds (e.g. tourists) and they may misinterpret the signal.
Source	Own experience, literature
Rationale	(Herman, 1996) (Jagne, 2004) (Smith, 2003) (Heimgärtner, 2014), ISO 7001:2007 – graphical symbols
Additional attributes	

UIREQ-ESR06-SP004-A11Y	
Description	The “smart space” signal must accommodate a target audience with disabilities
Priority	High
Dependency	UIREQ-ESR06-SP006-CONSENT, UIREQ-ESR06-SP001-SIGNAL
Risk	A blind or a deaf person may walk into a smart space unknowingly, thus their expectations of privacy can be violated
Source	Own experience, standards
Rationale	ISO 21542:2011 – accessibility and usability of the built environment
Additional attributes	

UIREQ-ESR06-SP005-GENUINE	
Description	The “smart space” signal must be verifiably genuine
Priority	High
Dependency	UIREQ-ESR06-SP001-SIGNAL
Risk	A spoofed signal will give people the wrong impression about the space they are walking into, making them assume that it has capabilities that it does not have in practice, leading to potential health risks or privacy violations. For example, if a store uses a sticker to say “this space is recording video”, the sticker can be replaced by a competitor with another sticker that says “is space is recording video and applying facial recognition to track you” to discourage people from entering the store. Visitors should be able to quickly determine that the signal is authentic.
Source	Own experience
Rationale	Such tricks are already used for financial scamming in Asia: https://www.techinasia.com/fake-qr-code-scams-china
Additional attributes	

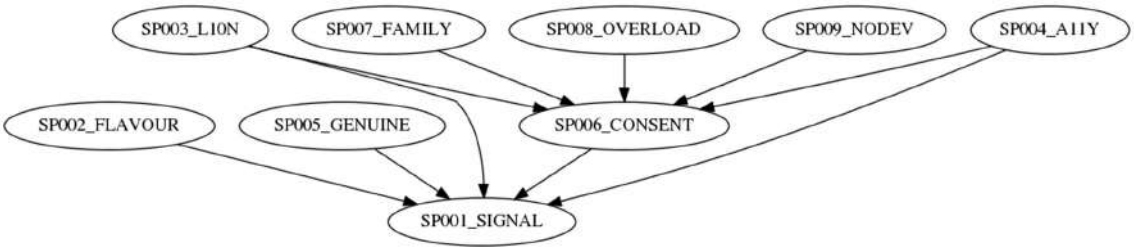
UIREQ-ESR06-SP006-CONSENT	
Description	The “smart space” must obtain consent from a person if personally identifying information is handled in ways explicitly mentioned in the regulations.
Priority	High
Dependency	UIREQ-ESR06-SP001-SIGNAL
Risk	If a smart space collects or otherwise uses personally identifying information (e.g. face recognition), it must only do so after obtaining consent from the person.
Source	Legislation
Rationale	GDPR Art.7 – request consent before collecting any data (except when the provisions of GDPR Art.6 apply). (EC, n.d.)
Additional attributes	

UIREQ-ESR06-SP007-FAMILY	
Description	The “smart space” should be able to retrieve consent information from custodians.
Priority	High
Dependency	UIREQ-ESR06-SP006-CONSENT
Risk	Minors walking around the environment can stumble upon smart spaces that will ask for consent, but in the case of a minor consent should be provided by parents (or legal custodians).
Source	
Rationale	• GDPR Art. 7 – request consent, Art. 8 – consent and minors • General usability matter that only becomes evident when one is a parent. TODO find reference
Additional attributes	

UIREQ-ESR06-SP008-OVERLOAD	
Description	The “smart space” should be able to retrieve consent information from adjacent smart spaces.
Priority	Medium
Dependency	UIREQ-ESR06-SP006-CONSENT
Risk	If a person will be asked to agree/disagree every 50 meters, this will desensitize them, paving the road for phishing and other types of scams
Source	
Rationale	TODO find study on Information overload, change blindness
Additional attributes	

UIREQ-ESR06-SP009-NODEV	
Description	The “smart space” should be able to retrieve consent information even when people carry no hardware (e.g. phone, wearable device) that would be able to serve as a UI
Priority	Medium
Dependency	UIREQ-ESR06-SP006-CONSENT
Risk	Tourists, old-school people and aliens should be able to blend into the environment without discrimination
Source	
Rationale	TODO find some non-discrimination law
Additional attributes	

2.5.2.1 Dependency Graph



Render it by pasting the code into https://www.planttext.com/

```
@startuml
digraph G {
    SP002_FLAVOUR -> SP001_SIGNAL
    SP005_GENUINE -> SP001_SIGNAL
    SP003_CULTURE -> SP001_SIGNAL, SP006_CONSENT
    SP004_A11Y -> SP001_SIGNAL, SP006_CONSENT
    SP007_FAMILY -> SP006_CONSENT
    SP008_OVERLOAD -> SP006_CONSENT
    SP009_NODEV -> SP006_CONSENT
    SP006_CONSENT -> SP001_SIGNAL
}
@enduml
```

2.5.3 User Interface Requirements IoT Devices

UIREQ-ESR06-IOT001-IMPORTANCE	
Description	Notifications from devices should be tagged with their level of importance, enabling people to filter out the less relevant ones and focus on the critical ones.
Priority	High
Dependency	
Risk	Too much verbosity produces a flood of data that is difficult to understand. It can also lead to notification fatigue and desensitize end-users.
Source	
Rationale	Personal experience derived from reading log-files of applications.
Additional attributes	

UIREQ-ESR06-IOT002-GROUP	
Description	Notifications from devices should be grouped together, to minimize the number of times a person is distracted.
Priority	Medium
Dependency	
Risk	Frequent interruptions make it difficult to keep focus.
Source	Personal experience, literature research
Rationale	• A person's self-assessed level of satisfaction depends, among other factors, on their ability to stay focused on their activity (Csikszentmihalyi, 1990) • Frequent interruptions can lead to alarm fatigue (Casey, 1993)
Additional attributes	

UIREQ-ESR06-IOT003-INCOGNITO	
Description	Devices should provide an *incognito switch*, where all data collection *and* transmission is disabled (microphone, camera, sensors, etc). A simple on/off switch provides that capability already, but it can only be toggled physically (and if you want it back on, you have to walk back to the device) and it involves side effects (e.g. the device has to boot, which imposes waiting periods)
Priority	Medium
Dependency	
Risk	
Source	Observation, own research on privacy perception
Rationale	
Additional attributes	

UIREQ-ESR06-IOT004-WIPE	
Description	Devices that preserve personally identifying information or any state information should include the capability to reset them to factory defaults
Priority	Medium
Dependency	
Risk	Devices sold after use can contain significant amounts of personal information that can be retrieved by their new owners
Source	Personal experience from forensics (Gubian, 2007) (Qiu, 2014)
Rationale	There are recovery mechanisms that retrieve information from SIM cards, or formatted partitions – it is expected that some traces of data can be recovered from discarded IoT devices. The interface of the device must provide the capability to wipe it.
Additional attributes	

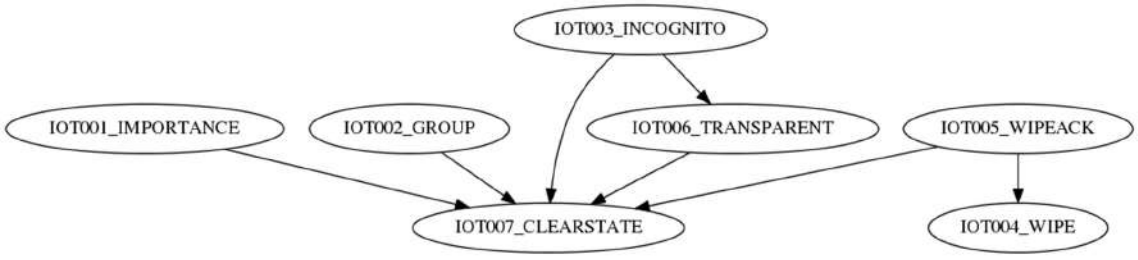
UIREQ-ESR06-IOT005-WIPEACK	
Description	The wipe capability must provide a clear indication of the fact that the device has been sanitized successfully and can be safely decommissioned.
Priority	Medium
Dependency	IOT005-WIPE, IOT007-CLEARSTATE
Risk	An end user who invokes a wipe procedure can be left wondering whether the wipe really worked, if they haven't turned off the device too soon, etc. An explicit marker will address their concern and reduce anxiety.
Source	Observations and my own research
Rationale	In an interview with a person who has sold (and wiped) their old smartphone, when asked whether they are sure the data are gone – they said yes. However, when asked how long the wiping process took, they said it was suspiciously fast (implying that for the large amounts of data they had, it should have taken longer). It is likely that the process was fast because the implementation simply wipes the encryption key of the data, not the actual data. Although this is secure, it causes a perception issue – end users believe that the data are still there. A better design would address the psychological side of the problem as well as the technical one.
Additional attributes	

UIREQ-ESR06-IOT006-TRANSPARENT	
Description	A device switched into incognito mode should make it clear even to a non-tech-savvy person that the device is obviously not recording anything.
Priority	Medium
Dependency	IOT003-INCOGNITO, IOT007-CLEARSTATE
Risk	If this is only expressed via a LED on the device, people will be anxious (what if the device is hacked? Is it *really* not recording?). A better solution is to include obvious mechanical signifiers (e.g. "camera lens is covered or closed" is better than "camera LED is off")

Source	Own experience, my own research
Rationale	Some people cover their web-camera with a slice of tape, because they do not trust the built-in LED indication - which can be hacked such that the camera is recording but the LED is off. My data collected from a current survey about IoT privacy perception indicates that people with home assistants (like Amazon Echo or Google Home) are aware of the `mute` button, but some consider the possibility that the device is still listening. Therefore, the *incognito switch* should be implemented in a way that makes it clear that the device is incapable of perceiving data (e.g. like a camera lens covered with tape) – this can be accomplished through designs that facilitate the development of simple and correct mental models (Norman, 2013)
Additional attributes	

UIREQ-ESR06-IOT007-CLEARSTATE	
Description	A device shall provide a clear indication of its current state.
Priority	Medium
Dependency	
Risk	
Source	
Rationale	
Additional attributes	

2.5.3.1 Dependency Graph



Render it by pasting the code into https://www.planttext.com/

```
@startuml
digraph G {
    IOT001_IMPORTANCE -> IOT007_CLEARSTATE
    IOT002_GROUP -> IOT007_CLEARSTATE
    IOT003_INCOGNITO -> IOT007_CLEARSTATE, IOT006_TRANSPARENT
    IOT004_WIPE
    IOT005_WIPEACK -> IOT004_WIPE, IOT007_CLEARSTATE
    IOT007_CLEARSTATE
    IOT006_TRANSPARENT -> IOT007_CLEARSTATE
}
@enduml
```

2.6 ESR-7 (UNI/FAU) Juan Quintero - The Role of Sealed Cloud Concept and Technology in User Acceptance and Usability of Privacy Applications

2.6.1 Scope

This section describes the user interface requirement for the project: The role of Sealed Cloud Concept and technology in user acceptance and usability of Privacy Applications. According to Fig. 1 they were chosen a Sealed Cloud (Jäger, Monitzer, Rieken, Ernst, & Nguyen, 2014), an user acceptance model (Benenson & Girard, 2015), and a Privacy respecting connected car in Insurance company's scenario to build a prototype and establish the role of Sealed Cloud concept and technology in user acceptance and usability.

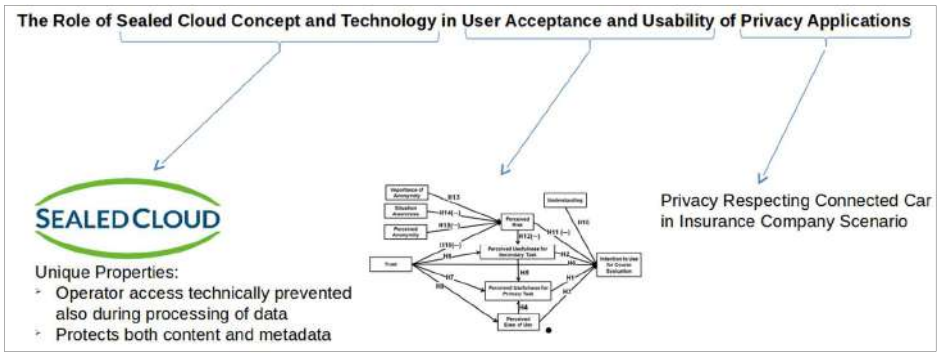


Fig.1. Explanation of ESR7 project title

The prototype will be a Privacy respecting platform that uses privacy-preserving analysis of data collected from the networked cars in the insurance company scenario. In the Fig.2 is represented a connected car system model, where networked cars drive through the streets using their sensors and cameras can get PII and non-PII data, such as: the car's position and speed (PII), road state and weather conditions (non-PII), energy consumption (PII), and other data. In Connected Car (Fig. 2), a huge amount of data should be stored, accessed, and processed according to the privacy regulations.

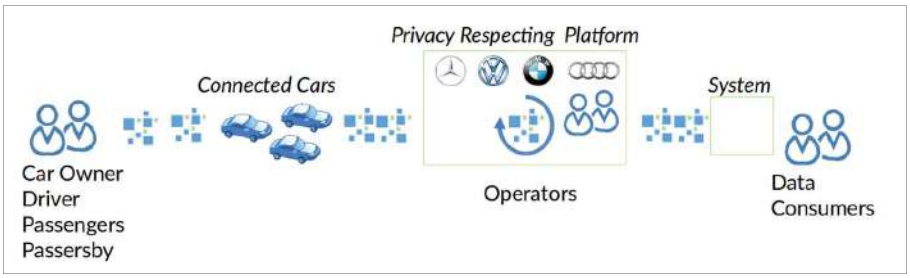


Fig.2. Connected Car system model

To standardize the name of actors in the user interface requirements and Insurance Company's scenario definition, the Table 1 defines a mapping between the system model and the terminology and definitions of GDPR (Union, 2016).

	Data Subject	Data Controller	Data Processor
Car Owner	yes	yes	
Driver	yes	yes	-
Passenger	yes	-	-
Passerby	yes	-	-
Operator	-	-	yes
Data Consumer	-	-	yes

Car Owner, Driver, Passengers, Passersby, Operators and third parties can be Data Consumers

Table.1. Mapping of Insurance company scenario to Terminology and Definitions of GDPR

In the Insurance Company scenario, the Data Processors (Insurance companies) could analyse the data of Data Subjects to find out behaviour patterns (driving style, speed, etc.) and reward him with new offers or discounts. This scenario requires PII and non-PII.

2.6.2 User Interface Requirements

UIREQ-ESR07-001-UserInformedConsent	
Description	The prototype shall provide a way to define and give the informed consents according to the usage purpose
Priority	High
Dependency	--
Risk	If the Informed consent is not according to the usage purpose, Data Subject can be exposed a privacy issue when his or her data will be used to process with different purposes. Data Processor can use the Data Subject's data to new purpose without an informed consent
Source	Legal regulations, Big data analytics, and Industry experiences
Rationale	"Consent should be given by a clear affirmative act establishing a freely given, specific, informed and unambiguous indication of the data subject's agreement to the processing of personal data relating to him or her, such as by a written statement, including by electronic means, or an oral statement. " (32) (Union, 2016) Lawfulness of processing. The data subject has given consent to the processing of his or her personal data for one or more specific purposes. Art 6 (1-a) (Union, 2016)
Additional attributes	Design Constraints: Mandatory accordingly GDPR regulation

UIREQ-ESR07-002-WithdrawingInformedConsent	
Description	The Data Subject shall always withdraw his or her informed consent, partially or totally
Priority	High
Dependency	UIREQ-ESR07-001-UserInformedConsent
Risk	If the Data Subject cannot withdraw his or her informed consent, partially or totally, his or her acceptance of the prototype would decrease

Source	Legal regulations
Rationale	Permit easy reversal of actions, Support internal locus of control (Shneiderman & Plaisant, 2004). Conditions for consent. The data subject shall have the right to withdraw his or her consent at any time… Art 7 (3) (Union, 2016)
Additional attributes	Design Constraints: Mandatory accordingly GDPR regulation Human Factors: Reliability, Satisfaction

UIREQ-ESR07-003-RequestErasePersonalData	
Description	The Data Subject shall request to the Data Controller that his or her personal data are erased partially or totally
Priority	High
Dependency	UIREQ-ESR07-001-UserInformedConsent
Risk	If the Data Subject cannot request that his or her personal data are erased partial or total his or her acceptance of the prototype would decrease
Source	Legal regulations
Rationale	User control and freedom: (Nielsen & Molich, NieMol90, 1990) Right to erasure. The data subject shall have the right to obtain from the controller the erasure of personal data concerning Art 17 (1) (Union, 2016)
Additional attributes	Design Constraints: Mandatory accordingly GDPR regulation Human Factors: Reliability

UIREQ-ESR07-004-PushNotification	
Description	The Data Subject shall have a way to be notified, according his or her preferences (on demand, periodic, or timing notice), when his or her personal data or informed consent are changed
Priority	Medium
Dependency	UIREQ-ESR07-002-WithdrawingInformedConsent, UIREQ-ESR07-006-ErasingPersonalData
Risk	If the Data Subject does not have a mechanism to be informed about changes in his or her personal data or informed consent, his or her acceptance of the prototype would decrease
Source	Legal regulations, Usability
Rationale	Design space of privacy notices (Schaub, Balebako, Durity, & Cranor, 2015) Visibility of system status (Nielsen & Molich, NieMol90, 1990)
Additional attributes	Design Constraints: Mandatory accordingly GDPR regulation Human Factors: Reliability

UIREQ-ESR07-005-ErasingPersonalData	
Description	The Data Controller shall erase the Data Subject's personal data supported on his or her request
Priority	High
Dependency	UIREQ-ESR07-003-RequestErasePersonalData

Risk	If the Data Controller cannot erase the Data Subject's personal data (partially or totally) supported on Data Subject's request, the user acceptance of the prototype would decrease and the legal regulation will be broken
Source	Legal regulations
Rationale	User control and freedom: (Nielsen & Molich, NieMol90, 1990) Right to erasure. Art 17 (Union, 2016)
Additional attributes	Design Constraints: Mandatory accordingly GDPR regulation

UIREQ-ESR07-006-TrackingPersonalData	
Description	The prototype shall allow that the Data Subject can track his or her personal data to know who and what are the purpose they are accessed
Priority	Medium
Dependency	UIREQ-ESR07-005-ErasingPersonalData
Risk	Data Processor would use the Data Subject's personal data for another purpose not authorized according to his or her informed consent
Source	Legal regulations
Rationale	Offer informative feedback: (Shneiderman & Plaisant, 2004) User control and freedom: (Nielsen & Molich, NieMol90, 1990) Transparent information, communication and modalities for the exercise of the rights of the data subject. Art 12 (Union, 2016)
Additional attributes	Design Constraint: GDPR regulation Usability: Usable Transparency

UIREQ-ESR07-007-StoringRawData	
Description	The prototype shall allow that the Data Controller can get and store the Data Subject's raw data
Priority	High
Dependency	--
Risk	The connection between the Data Controller and the Data Subject would break and the Data Controller will store data inconsistent
Source	Data persistence, Data integrity
Rationale	Visibility of system status: (Nielsen & Molich, NieMol90, 1990)
Additional attributes	Design Constraint: Data Integrity

UIREQ-ESR07-008-MonitoringInStoredRawData	
Description	The prototype shall allow to the Data Controller check that stored raw data are corresponding with an informed consent
Priority	High
Dependency	--
Risk	Some stored raw data would not have an informed consent and they would be processed without the data subject´s authorization
Source	Legal regulations
Rationale	Offer informative feedback, offer simple error handling: (Shneiderman & Plaisant, 2004)

	Visibility of system status: (Nielsen & Molich, NieMol90, 1990) Conditions for consent. Art 7 (1) (Union, 2016)
Additional attributes	Design Constraint: GDPR regulation Usability: Usable Transparency

UIREQ-ESR07-009-ExecutingQuery	
Description	The Data Processor shall see the Data Subject's information according to the informed consent
Priority	High
Dependency	UIREQ-ESR07-001-UserInformedConsent, UIREQ-ESR07-007-StoringRawData
Risk	Data Processor would get the Data Subject's information without a corresponding informed user consent and the data subject´s privacy will be broken
Source	Legal regulations, Industry concern
Rationale	Offer informative feedback, offer simple error handling: (Nielsen & Molich, NieMol90, 1990) Flexibility and efficiency of use, Aesthetic and minimalist design: (Nielsen & Molich, NieMol90, 1990)
Additional attributes	Human Factors: Performance, Effectiveness

2.7 ESR-8TBD (TAU) Yefim Shulman - Modeling Responses to Privacy-related Indications

2.7.1 Scope

The current document is created to elaborate on and specify higher level user interface requirements for the project "Modelling Responses to Privacy-related Indications". The goal of the project – in the part related to designing the User Interface – is to develop a model of the user's decision making regarding the performance of actions that may impact privacy. In that sense privacy is considered as a function of:

- the disclosed information,
- the (perceived) identity of whoever will have access to the information,
- the context in which the information is provided,
- the user's individual characteristics,
- and indications from the system pointing to the possible privacy implications of a user action.

The developed model is to be validated among other things through laboratory experiments deemed to assess the effects of different variables on user decisions. Said experiments are to be conducted employing certain software system, hence interacting with subjects (users, testees) via GUI, for which the following requirements have been developed.

2.7.2 User Interface Requirements

UIREQ-ESR08-000-CLEARCOM	
Description	The system at any given stage of interacting with the subjects shall communicate with the subjects in plain language avoiding ambiguous and misleading phrasing
Priority	High
Dependency	None
Risk	Basic requirement: consistence and conventional language
Source	Observation

Rationale	The subjects should not struggle to understand or being put off by any piece of information provided during the experiment (Nielsen J. , Heuristic Evaluation, 1994)
Additional attributes	--

UIREQ-ESR08-001-INDICATION	
Description	The system shall present the subjects with privacy-related indications and register the subjects' responses in a subsequent randomized order during the course of the experiment.
Priority	High
Dependency	UIREQ-ESR08-000-CLEARCOM
Risk	If the subjects do not receive said indications, they would not be able to provide response in both explicit and implicit form.
Source	Rationale of the project: the validation method derived from the essence of the scope of the project
Rationale	The requirement is drawn from the goal of the project. Basic requirement: no testing results and validation can be gained without that prerequisite
Additional attributes	--

UIREQ-ESR08-002-CONTENT	
Description	Privacy-related indications shall • contain information about response needed (if needed) from the subjects – in a variety of formats; • and state clearly, imply or conceal possible ways of use of their private information.
Priority	High
Dependency	UIREQ-ESR08-000-CLEARCOM, UIREQ-ESR08-001-INDICATION
Risk	If the subjects are not exposed to a certain "spectrum" of indications varying in content, detail and format, they will not be able to demonstrate the necessary variety of responses to correspond sufficiently to the scope of the experiment
Source	Observation
Rationale	The content presented and the way of presentation is the nature of the experiment determining the usefulness and applicability of the expected results. The responses formats and content, as well as additional attributes, informing (or abstaining to inform) the subjects about the future use of their personal information, will be determined in a future study that will measure privacy attitudes and behaviour of the users. (ISO 9241-210: 2010, 2010) – the principles for user experience design (Nielsen J. , Heuristic Evaluation, 1994)– consistency and standards; and match between system and the real world.
Additional attributes	--

UIREQ-ESR08-003-FAMILIARITY	
Description	Privacy-related indications and their content shall be presented in forms which are common to subjects (i.e. being ubiquitously represented in existing software applications such as social networking services, online

	commerce services and (or) mobile, desktop and internet-based software applications)
Priority	High
Dependency	UIREQ-ESR08-001-INDICATION, UIREQ-ESR08-002-CONTENT
Risk	If a privacy-related indication is shown in a form unbeknown to users from their previous experience, it may lead to skewed or biased results. This may happen due to the fact that the subjects would have to undertake the tasks with more effort, engaging stronger focus thus invoking higher concentration. The opposite may hold true as well. The subjects may be discouraged, loose interest in and concentration on the task. Both situation can result in irregularities in subjects' behaviour (in comparison to usual real-life behaviour) lowering the validity of the model.
Source	Nielsen, 1994 – partially from matching "system and the real world"
Rationale	Time perception is altered with increase in complexity of stimuli and (or) increase in effort needed to perform a task what can influence decision making (Shiffmann, 2001).
Additional attributes	--

UIREQ-ESR08-004-WHEREAMI	
Description	The system shall clearly state at which stage of the process it currently manifests itself.
Priority	High
Dependency	UIREQ-ESR08-000-CLEARCOM
Risk	If the system does not positively establish its current status, the subjects might be unaware of what is going on, should they be interacting with the system and whether the interactions are possible at all
Source	(Nielsen J. , Heuristic Evaluation, 1994)
Rationale	(Nielsen J. , Usability engineering, 1993) – visibility and system status (ISO 9241-210: 2010, 2010) – the principles for user experience design
Additional attributes	--

UIREQ-ESR08-005-EXPLAINAGAIN	
Description	Instructions and help messages should be easily accessible (visible or retrievable "in one click") by the subjects during the interaction (experiment)
Priority	High
Dependency	UIREQ-ESR08-000-CLEARCOM
Risk	If instructions and help messages cannot be intuitively obtained, it may distract the subjects, force them to address other subjects or experimentator for advice, thusly distracting other subjects and bringing unwanted level of interference to the process
Source	(Nielsen & Molich, NieMol90, 1990)
Rationale	(Nielsen J. , Usability engineering, 1993)
Additional attributes	--

UIREQ-ESR08-006-PRECISENESS	
Description	System prompts and messages shall not contain extra (beyond necessary) explanatory and (or) technical information which is irrelevant to the subjects during the interaction with the system (experiment)
Priority	High
Dependency	UIREQ-ESR08-000-CLEARCOM, UIREQ-ESR08-004-WHEREAMI, UIREQ-ESR08-005-EXPLAINAGAIN
Risk	The subjects should be exposed to the amount of information in precise, but not exhaustive manner, to avoid any possibility for attention (thought processing) overload. Additionally, these precautions should be taken in order to avoid occasional disclosing of essential information about the experimentation detail to the subjects as so as it can result in alteration in the subjects' behaviour (e.g., to do what they think the experimentator wants as well as do the opposite on purpose)
Source	Literature review
Rationale	Whereas high perceptual load may reduce distracter interference, working memory load or dual-task coordination load increases distracter interference (Lavie, Hirst, De Fockert, & Viding, 2004)
Additional attributes	--

UIREQ-ESR08-007-WHATDYWANT	
Description	The system shall clearly state what (if anything) is required from the subjects at any given moment during their interaction (experiment). The system shall clearly state that the subject shall remain idle when no user action is required.
Priority	High
Dependency	UIREQ-ESR08-000-CLEARCOM, UIREQ-ESR08-002-CONTENT, UIREQ-ESR08-004-WHEREAMI, UIREQ-ESR08-005-EXPLAINAGAIN, UIREQ-ESR08-006-PRECISENESS
Risk	If the instructions are not presented beforehand or at the same time when the action is or is not needed (which also should be done in a clear fashion), the subjects might struggle with accomplishing the interaction (experiment)
Source	Observation
Rationale	(Nielsen J. , Heuristic Evaluation, 1994) (ISO 9241-210: 2010, 2010)– the principles for user experience design
Additional attributes	--

UIREQ-ESR08-008-OOPSPROOF	
Description	The system should present messages, prompts, privacy-related indications and interactive elements (e.g., buttons, boxes, customizable fields) in such a way that subjects' action performed in accordance to the experiment instructions would not lead to an invalid action.
Priority	High
Dependency	UIREQ-ESR08-000-CLEARCOM, UIREQ-ESR08-001-INDICATION
Risk	If users' actions, performed according to the instructions, result in the system's misbehaviour, users' attention and mental workload capacity

	might be hindered, and attitudes regarding conduct and compliance with the course of the experiment can be swayed, for which it is technologically inconceivable to entirely account. Unless this requirement is implemented, there would emerge a necessity of developing more particular system requirements to account for each of the plausible errors.
Source	Observation
Rationale	(Nielsen J. , Heuristic Evaluation, 1994) “error prevention” (Nielsen J. , Usability engineering, 1993)– consistency and standards
Additional attributes	--

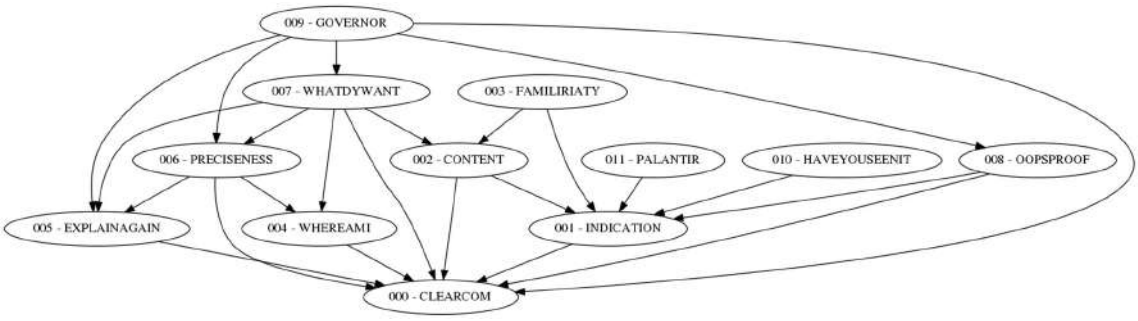
UIREQ-ESR08-009-GOVERNOR	
Description	In case of any unconventional behaviour (i.e., the one that was not envisaged), the system should present the subjects with error messages containing stepwise information on how to proceed
Priority	High
Dependency	UIREQ-ESR08-000-CLEARCOM, UIREQ-ESR08-005-EXPLAINAGAIN, UIREQ-ESR08-006-PRECISENESS, UIREQ-ESR08-007-WHATDYWANT, UIREQ-ESR08-008-OOPSPROOF
Risk	If a constructive solution is not provided to the subjects, it may lead to confusion, anxiety and may affect the subjects’ decision making
Source	General industry convention
Rationale	Being a logical addition to UIREQ-ESR08-008-OOPSPROOF, (Nielsen J. , Heuristic Evaluation, 1994) “help users […] recover from errors”
Additional attributes	--

UIREQ-ESR08-010-HAVEYOUSEENIT	
Description	The system should be able to ensure that the privacy-related indication has been presented to the subjects meaning that the privacy-related indication has not been skipped by mistake made on the system’s part
Priority	Medium
Dependency	UIREQ-ESR08-001-INDICATION
Risk	If the interactions’ (experiment’s) results lack the data on whether the indications were properly offered to the subjects item- and time-wise, the analysis of the data may lead to erroneous conclusions
Source	Assumption made a priori
Rationale	This requirement may provide further insight on the sample quality and may help to devise suggestion on how to refine the data
Additional attributes	--

UIREQ-ESR08-011-PALANTIR	
Description	The system may be able to track and record the metadata on subjects’ performance in order to discriminate between cases when the subjects give different level attention to different messages or do not commit to the interaction at all
Priority	Medium
Dependency	UIREQ-ESR08-001-INDICATION

Risk	If metadata is not collected for further analysis of the results, the quality of the model and potential projects' performance will be affected in several unwanted ways (see Rationale)
Source	Industry best practices
Rationale	Lack of data for potential re-calibration of the model resulting in inability to improve the model; worse performance of the final model resulting in poorer quality of the project's final result and evaluation; etc. – these are justification thoughts on the matter
Additional attributes	Should be thought through more carefully in more detail

2.7.2.1 Dependency Graph



[@startuml
digraph Stephen {
"001 - INDICATION" -> "000 - CLEARCOM"
"002 - CONTENT" -> "000 - CLEARCOM"
"002 - CONTENT" -> "001 - INDICATION"
"003 - FAMILIRIATY" -> "001 - INDICATION"
"003 - FAMILIRIATY" -> "002 - CONTENT"
"004 - WHEREAMI" -> "000 - CLEARCOM"
"005 - EXPLAINAGAIN" -> "000 - CLEARCOM"
"006 - PRECISENESS" -> "000 - CLEARCOM"
"006 - PRECISENESS" -> "004 - WHEREAMI"
"006 - PRECISENESS" -> "005 - EXPLAINAGAIN"
"007 - WHATDYWANT" -> "000 - CLEARCOM"
"007 - WHATDYWANT" -> "002 - CONTENT"
"007 - WHATDYWANT" -> "004 - WHEREAMI"
"007 - WHATDYWANT" -> "005 - EXPLAINAGAIN"
"007 - WHATDYWANT" -> "006 - PRECISENESS"
"008 - OOPSPROOF" -> "000 - CLEARCOM"
"008 - OOPSPROOF" -> "001 - INDICATION"
"009 - GOVERNOR" -> "000 - CLEARCOM"
"009 - GOVERNOR" -> "005 - EXPLAINAGAIN"
"009 - GOVERNOR" -> "006 - PRECISENESS"
"009 - GOVERNOR" -> "007 - WHATDYWANT"
"009 - GOVERNOR" -> "008 - OOPSPROOF"
"010 - HAVEYOUSEENIT" -> "001 - INDICATION"
"011 - PALANTIR" -> "001 - INDICATION"
}
@enduml]

2.8 ESR-10 (UNI/FAU) Lamya Abdullah - Adaptive Data Privacy for Smart Environments

2.8.1 Scope

Smart environment provides information about user's surroundings and detailed statuses. The main goal of such applications is to increase opportunities and provide accurate user-related services. But that comes on a cost on the user's privacy. The below are high-level requirements for a smart

environment system that shall allow the user to be involved in defining preferred privacy. These requirements are subject to change based on the application domain and type of services.

2.8.2 User Interface Requirements

UIREQ-ESR10-001- User Profile - create	
Description	The system shall allow the end user to create a profile during the service registration process that consists of the required information for the application domain.
Priority	High
Dependency	
Risk	This is basic requirement for the system to develop user privacy profile.
Source	Functional Requirements Analysis phase of the project
Rationale	
Additional attributes	Design Constraints: ToDo; related to the amount of required data

UIREQ-ESR10-002- User preferences -	
Description	The system shall require the user to add preferences on the level of data categories, not only general profile level, in flexible and consistent mode.
Priority	High
Dependency	
Risk	If the user did not set preferences for privacy control and sharing
Source	(Fischer-Hübner, 2011)
Rationale	Functional privacy-related system requirement.
Additional attributes	Design Constraints: ToDo whether it is should be mandatory for the service to keep running

UIREQ-ESR10-003- Show collected data categories	
Description	The system shall clearly provide the user information of the collected data and it's related policy.
Priority	High
Dependency	
Risk	If the user is not able to see such details then the profile and preferences update will be mislead.
Source	Observation
Rationale	Visibility of system status: to keep the user informed (Fischer-Hübner, 2011)
Additional attributes	Design Constraints: that is based on the data categorisation which shall be carefully designed and abstracted to be shown to the user.

UIREQ-ESR10-004- User Profile – update	
Description	The system shall provide the user the ability to update the profile.
Priority	High

Dependency	UIREQ-ESR10-001- User Profile – create, UIREQ-ESR10-003- Show collected data categories
Risk	If the user is not able to update the profile then both system functionality and user data privacy will not be maintain.
Source	Observation and analysis
Rationale	
Additional attributes	Design Constraints: this will be defined in relation to specifications of how often profile updates are required.

UIREQ-ESR10-005- preferences notification.	
Description	The system shall frequently notify the user with the current preferences in relation to privacy policy changes.
Priority	Medium
Dependency	UIREQ-ESR10-001- Show collected data categories, UIREQ-ESR10-002- User preferences,
Risk	Not Defined Yet
Source	(Schaub, Balebako, Durity, & Cranor, 2015) Nielsen, J. (1994). Heuristic Evaluation. In J. Nielsen, Usability Inspection Methods.
Rationale	Visibility of system status
Additional attributes	Design Constraints: Depends on what privacy policy to be shared with users (considering non-technical users)

2.9 ESR-11 (UCL) Alexandros Mittos - Secure and Privacy-Preserving Personal Genomic Testing

2.9.1 Scope

The tables below describe the high-level user interface requirements of a privacy-preserving personal genomic testing framework where the user/patient is able to observe and regulate how her genomic data is being used and by whom.

2.9.2 User Interface Requirements

UIREQ-ESR11-001-Access Control	
Description	The user must specify her consent preferences before third parties can access her genome
Priority	High
Dependency	
Risk	The user may experience a privacy breach if her genome gets accessed without her consent. Repeating accesses can infer information about one's genome other than the absolute required.
Source	Literature on genomic privacy, privacy legislation, healthcare legislation, GDPR
Rationale	Privacy and security. The user should know and control who accesses her data and why.
Additional attributes	

UIREQ-ESR11-002-Consent	
Description	The artefact shall indicate when the user's data is being processed, for what reason, and by whom, unless previously consented to
Priority	High
Dependency	
Risk	If the user is not aware of, and consenting to, what her/his data is being used for then her/his consent will have been breached
Source	Literature on genomic privacy, privacy legislation, healthcare legislation, GPDR
Rationale	Visibility. The user should always know who accesses her data and why.
Additional attributes	

UIREQ-ESR11-003-Transparency	
Description	The artefact shall display who is accessing the user's data and for what purposes
Priority	High
Dependency	UIREQ-ESR11-002-Transparency
Risk	The user may not agree with the privacy policies of the entity accessing her data
Source	Literature on genomic privacy, privacy legislation, healthcare legislation, GPDR
Rationale	• Visibility. The user should always know who accesses her data and why. • Sensitivity of health data. i.e. the user might not want an entity to analyse her genome for certain reasons
Additional attributes	

UIREQ-ESR11-004-History	
Description	The artefact shall display a history of the entities accessing the user's data
Priority	Low
Dependency	
Risk	The user might not remember previous access and her decision making might be affected
Source	
Rationale	It should be clear to the user who accessed her data in the span of years
Additional attributes	

2.10 ESR-12 (UCL) Mark Warner - Effective cost-benefit signalling in healthcare data disclosure decision-making

2.10.1 Scope

Disclosing sensitive healthcare data across complex technologies can create uncertainty for users. Effective privacy trust systems rely on proving users with clear indicators of value proposition alongside personal data management controls. These user requirements are provided for healthcare technologies requiring end-user information disclosure.

2.10.2 User Interface Requirements

UIREQ-ESR12-001-FEEDBACK	
Description	The technology will promote privacy awareness, providing the user with details on who has access to their data, and for what purpose, integrated within the common interaction areas of the system (i.e. not hidden).
Priority	High
Dependency	UIREQ-ESR12-003-APROPRIATE-FLOW
Risk	• Uncertainty over who is aware of the user's health status may act as a stressor, effecting mental and physical wellbeing. • Users unaware of who has access to their healthcare status, may be less able to manage how they present their identity across different online environments. • Creating transparency on access in a separate screen risks removing the visibility of access from the user. • Users without awareness of who has access to their data cannot be alerted to inappropriate management of their data
Source	(Xu, Wang, & Grossklags, 2012) (Wagner, He, Rosenberg, & Janicke, 2016) (Nissenbaum, 2009)
Rationale	GDPR – Article 12
Additional attributes	

UIREQ-ESR12-002-PERSONAL	
Description	Automated communication sent to users will include a person's name e.g. 'Sarah', 'John'.
Priority	High
Dependency	
Risk	Communications sent without a name may reduce user response rates.
Source	Observation – Evaluation of the automated notification system in a UK sexual health clinic
Rationale	interaction
Additional attributes	

UIREQ-ESR12-003-APROPRIATE-FLOW	
Description	Users will be able to mitigate data access and usage they perceive as being inappropriate
Priority	High
Dependency	UIREQ-ESR12-001-FEEDBACK
Risk	If a user's healthcare status was used or disclosed to someone they had not intended or anticipated, this may result in privacy violations, reducing user acceptance of the technology.
Source	(Wagner, He, Rosenberg, & Janicke, 2016) (Nissenbaum, 2009)
Rationale	GDPR Article 5 – Principles related to processing of personal data
Additional attributes	

UIREQ-ESR12-004-AUTONOMY	
Description	The technology will not fully automate decision which directly affect them, instead engaging with users in a constraining way, ensuring not to overwhelm the user.
Priority	High
Dependency	
Risk	• Loss of control over actions that have a direct effect on users • Reduced visibility of the technologies value, potential increasing privacy concerns by reducing the benefit in cost/benefit models.
Source	Yang, R., & Newman, M. W. (2013, September). Learning from a learning thermostat: lessons for intelligent systems for the home. In *Proceedings of the 2013 ACM international joint conference on Pervasive and ubiquitous computing* (pp. 93-102). ACM.
Rationale	interaction
Additional attributes	

UIREQ-ESR12-005-SECONDARY-USE	
Description	The technology will provide users with informed consent when self-disclosed or meta-data is subjected to secondary use. To constrain the number of user request interruptions, the technology will provide the user with broad secondary use permissions i.e. Identifiable data can be used for X, Non-identifiable data can be used for X, identifiable X data must never be shared with X.
Priority	High
Dependency	
Risk	• Non-consented secondary use of personal information may lead to reduced trust and a reducing in future disclosure • Requests for permission on each item of data will overload the users leading to disengagement.
Source	Observation
Rationale	GDPR Article 7 – Conditions for consent
Additional attributes	

UIREQ-ESR12-006-DATA-LIFE	
Description	The technology will provide the user with access to a data-life stream, associated to all meta-data generated by the technology. Meta-data that is generated about a user, resulting in functionality such as entity suggestions (e.g. People that you may know), will contain an easy to access data-life stream, increasing user transparency.
Priority	High
Dependency	UIREQ-ESR12-001-FEEDBACK UIREQ-ESR12-003-APROPRIATE-FLOW UIREQ-ESR12-005-SECONDARY-USE UIREQ-ESR12-007-DATA-LIFE-CONTROL
Risk	Failure to provide the user with details about how meta-data about them was created, will reduce data transparency and a user's ability to manage how their identity is presented to others.
Source	(Cavoukian & Jonas, 2012)
Rationale	GDPR –Article 13
Additional attributes	

UIREQ-ESR12-007-DATA-LIFE-CONTROL	
Description	The user will be able to control the meta-data that is generated from self-disclosed data.
Priority	High
Dependency	UIREQ-ESR12-005-DATA-LIFE
Risk	Failure to provide control over the way in which meta-data is generated, risks reducing a user's ability to manage how their identity is presented to others.
Source	(Nielsen J. , Heuristic Evaluation, 1994) Feedback
Rationale	GDPR – Section 2, Article 13 (2) (G)
Additional attributes	

2.11 ESR-13 (VDS/UCL) Andreas Gutmann - Privacy Preserving Transaction Authentication for Mobile Devices

2.11.1 Scope

Secure authentication of the intention of an activity, also known as transaction authentication, relies on a user having ability and legitimacy to authenticate, and being able to confirm that an action he is about to authenticate matches with his intention. The user interface requirements here are concerned with the I/O of a transaction authentication artefact at the intersection with its user.

2.11.2 User Interface Requirements

UIREQ-ESR13-001-SystemStatus	
Description	The artefact shall display the system status and possible operations in a user-understandable manner
Priority	high

Dependency	
Risk	If the user is not aware of the current system status or the actions he could possibly take, he won't be able to correctly operate the artefact.
Source	observation
Rationale	Visibility of system status, (Nielsen J. , Heuristic Evaluation, 1994)
Additional attributes	

UIREQ-ESR13-002-Warning	
Description	The artefact shall indicate system errors and security warnings in a user-understandable manner
Priority	high
Dependency	UIREQ-ESR13-001
Risk	If the user is not aware of errors and security warnings, he won't be able to correctly and securely operate the artefact.
Source	observation
Rationale	Visibility of system status, error prevention, (Nielsen J. , Heuristic Evaluation, 1994)
Additional attributes	

UIREQ-ESR13-003-WarningReaction	
Description	The artefact shall clearly communicate to the user which actions he could take in case of an (artefact related) error or security warning, and their consequences.
Priority	high
Dependency	UIREQ-ESR13-002
Risk	If the user is not aware of the actions he could possibly take, and their consequences, he won't be able to recover in a secure manner.
Source	observation
Rationale	Error recovery, (Nielsen J. , Heuristic Evaluation, 1994)
Additional attributes	

UIREQ-ESR13-004-StatusOpenTransaction	
Description	The artefact could communicate to the user the state of any open transactions and the moment a transaction has been completed.
Priority	low
Dependency	UIREQ-ESR13-001, UIREQ-ESR13-002
Risk	If the user is not aware of transactions that haven't been completed, he might fail to authenticate them. If the user is not made aware that transactions have been completed, he might be distressed the not receiving feedback of *task completion*.
Source	observation
Rationale	Visibility of system status, error prevention

Additional attributes	

UIREQ-ESR13-005-ResetCredentials	
Description	The artefact should provide and/or support a secure, efficient, and satisfying method to reset and to change authentication credentials.
Priority	Medium
Dependency	UIREQ-ESR13-001
Risk	If the user forgot the transaction authentication credentials or doesn't consider them being secret anymore, he should be able to reset or change them with a reasonably convenient and secure method.
Source	observation
Rationale	Error recovery, security, (Jobush & Oldehoeft, 1989)
Additional attributes	

UIREQ-ESR13-006-UnsuccessfulLogins	
Description	The artefact should, upon successful authentication, display the time of the previously most recent successful authentication and the number of unsuccessful authentication attempts since then.
Priority	Medium
Dependency	
Risk	Unsuccessful authentication attempts that to not stem from the legitimate user are strong indicators that another person tried to misuse the artefact. The legitimate user should be made aware of this to potentially identify and mitigate security threats.
Source	observation
Rationale	Security, (Jobush & Oldehoeft, 1989)
Additional attributes	

UIREQ-ESR13-007-DetailsTransaction	
Description	The artefact shall provide the ability to access the full details of a transaction.
Priority	High
Dependency	UIREQ-ESR13-001
Risk	Users need to be able to access the full transaction details in order to verify their correctness.
Source	observation
Rationale	Security
Additional attributes	

3 Conclusion

The preliminary considerations of each ESR already show that user interfaces play an important role in any type of product, system or service. Although all projects are in an early stage, taking high level user interface requirements already into consideration is of high value for the later stages. Many of the ESRs base their user interface requirements considerations on well-established heuristics, like defined by (Nielsen & Molich, NieMol90, 1990).

In terms of the human centred design approach (International Organization for Standardization, 2010), leading to products, systems and services that are usable and having an adequate user experience the user interface requirements will change / evolve over time.

5 References

(ISO), I. S. (2009). DIS, I. 9241-210: 2010. Ergonomics of human system interaction-Part 210: Human-centred design for interactive systems.

Acquisti, A. B. (2015). Privacy and Human Behavior in the Age of Information. *Science, 347(6221)*, 509–514.

Android. (2017). *Keeping Your App Responsive*. Retrieved 2017, from Android Developers: https://developer.android.com/training/articles/perf-anr.html

Balebako, R., Jung, J., Lu, W., Cranor, L. F., & Nguyen, C. (2013). "Little Brothers Watching You": Raising Awareness of Data Leaks on Smartphones. *Proceedings of the Ninth Symposium on Usable Privacy and Security* (p. 11). ACM.

Benenson, Z., & Girard, A. (2015). User Acceptance Factors for Anonymous Credentials: An Empirical Investigation. *Annu. Work. Econ. Inf. Secur.*, (pp. 1-33).

Benisch, M. K. (2011). Capturing location-privacy preferences: Quantifying accuracy and user-burden tradeoffs. . *Personal and Ubiquitous Computing, 15(7)*, 679–694.

Benyon, D. (2010). *Designing interactive systems A comprehensive guide to HCI and interaction design.*

Brandimarte, L. A. (2013). Misplaced Confidences: Privacy and the Control Paradox. . *Social Psychological and Personality Science, 4(3)*, 340–347.

Bruening, P. J. (North Carolina Journal of Law & Technology, (June)). Through a Glass Darkly : From Privacy Notices to Effective Transparency. . *2015*, 1–46.

Casey, S. M. (1993). *Set Phasers on Stun: And Other True Tales of Design, Technology, and Human Error* .

Cavoukian, A., & Jonas, J. (2012). *Privacy by design in the age of big data.* Ontario, Canada: Information and Privacy Commissioner of Ontario, Canada.

Chiles, J. R. (2008). *Inviting Disaster: Lessons From the Edge of Technology.*

Csikszentmihalyi, M. (1990). *Flow: The Psychology of Optimal Experience.*

Dix, A. F. (2004). *Human-Computer Interaction. Third edition (Third).* Essex : Pearson Educational Limited.

EC. (n.d.). *General Data Protection Regulation*. Retrieved from https://gdpr-info.eu/.

ENISA. (2013). *On the security, privacy and usability of online seals. .* ENISA - European Union Agency for Network and Information Security.

EU. (2016). *REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL* . Official Journal of the European Union,.

Fischer-Hübner, S. A. (2011). Towards Usable Privacy Enhancing Technologies: Lessons Learned from the PrimeLife Project. . *Privacy and Identity Management in Europe for Life*.

Fischer-Hübner, S., Angulo, J., Karegar, F., & Pulls, T. (2016). Transparency, Privacy and Trust – Technology for Tracking and Controlling My Data Disclosures: Does This Work? *IFIP International Conference on Trust Management* (p. 11). Springer.

Galitz, W. O. (2002). *The Essential Guide to User Interface Design.* New York, US: John Wiley & Sons, Inc.

Geven, A. P. (2007). Experiencing real-world interaction: results from a NFC user experience field trial. *Proceedings of the 9th international conference on Human computer interaction with mobile devices and services*, 234-237.

Gubian, A. S. (2007). SIM and USIM Filesystem: a Forensics Perspective. *ACM Symposium on Applied Computing*.

Heimgärtner, R. (2014). ISO 9241-210 and Culture? – The Impact of Culture on the Standard Usability Engineering Process. *Design, User Experience, and Usability*.

Herman, L. (1996). Towards effective usability evaluation in Asia: cross-cultural differences. *IEEE*.

Hsieh, G., Tang, K. P., Low, W. Y., & Hong, J. I. (2007). Field deployment of IMBuddy: A study of privacy control and feedback mechanisms for contextual IM. *Lecture Notes in Computer Science.*

International Organization for Standardization. (1998). *Guidance on usability.* ISO.

International Organization for Standardization. (2006). *Ergonomics of human-system interaction—Part 110: Dialogue principles.* ISO. ISO copyright office.

International Organization for Standardization. (2010). *Ergonomics of human-system interaction—Part 210: Human-centered design for interactive systems.* ISO. ISO copyright office.
ISO 9241-210: 2010. (2010). Ergonomics of human system interaction-Part 210: Human-centred design for interactive systems. Switzerland: International Standardization Organization (ISO).
ISO/IEC/IEEE. (2011). *Systems and software engineering — Life cycle processes — Requirements engineering.* ISO copyright office.
Jagne, J. (2004). CROSS-CULTURAL INTERFACE DESIGN STRATEGY. *Interaction Design Centre, technical report*.
Jobush, D. L., & Oldehoeft, A. E. (1989). A survey of password mechanisms: Weaknesses and potential improvements. Part 1. *Computers & Security, 8*(7), 587 - 604.
Johnson, E. J. (2002). Defaults, Framing and Privacy: Why Opting In-Opting Out. *Marketing Letters, 13(1)*, 5-15.
Johnson, J. (2010). *Designing with the Mind in Mind, Second Edition: Simple Guide to Understanding User Interface Design Guidelines.* Burlington, MA, US: Morgan Kaufmann.
Jäger, H., Monitzer, A., Rieken, R., Ernst, E., & Nguyen, K. (2014). Sealed Cloud – A Novel Approach to Safeguard against Insider Attacks. In *Trusted Cloud Computing* (pp. 15-34). Springer International.
Kani-Zabihi, E., & Helmhout, M. (2012). Increasing Service Users' Privacy Awareness by Introducing On-Line Interactive Privacy Features. In P. Laud, *Information Security Technology for Applications: 16th Nordic Conference on Secure IT Systems, NordSec 2011, Tallinn, Estonia, October 26-28, 2011, Revised Selected Papers.* Springer.
Kelley, P. G., Hankes Drielsma, P., Sadeh, N., & Cranor, L. F. (2008). User-controllable Learning of Security and Privacy Policies. *Proceedings of the 1st ACM Workshop on Workshop on AISec* (pp. 11–18). ACM.
Lavie, N., Hirst, A., De Fockert, J. W., & Viding, E. (2004). Load theory of selective attention and cognitive control. *Journal of Experimental Psychology: General, 133(3)*, 339-354.
Nielsen, J. (1993). *Usability engineering.* Cambridge, MA: Academic Press, Inc.
Nielsen, J. (1994). Heuristic Evaluation. In J. Nielsen, *Usability Inspection Methods.*
Nielsen, J. (1994). Heuristic Evaluation. In J. Nielsen, J. Nielsen, & R. L. Mack (Eds.), *Usability Inspection Methods* (pp. 25-62). New York, NY, USA: John Wiley & Sons, Inc.
Nielsen, J. (1994). *Usability Inspection Methods.* Bellcore.
Nielsen, J., & Molich, R. (1990). Heuristic Evaluation of User Interfaces. *Proceedings of the ACM 1990 International Conference on Human Factors in Computing Systems*, (pp. 249-256). Seattle.
Nissenbaum, H. (2009). *Privacy in context: Technology, policy, and the integrity of social life.* Stanford University Press.
Norman, D. (2013). *The design of everyday things.*
Qiu, W. (2014). A New Approach to Multimedia Files Carving.
Raskin, J. (2011). *The humane interface: new directions for designing interactive systems.* Boston.
Reeder, R. W., Kelley, P. G., McDonald, A. M., & Cranor, L. F. (2008). A User Study of the Expandable Grid Applied to P3P Privacy Policy Visualization. *Proceedings of the 7th ACM Workshop on Privacy in the Electronic Society* (pp. 45–54). ACM.
Sadeh, N., Hong, J., Cranor, L., Fette, I., Kelley, P., Prabaker, M., & Rao, J. (2009). Understanding and capturing people's privacy policies in a mobile social networking application. *Personal and Ubiquitous Computing, 13*(6), 401–412.
Schaub, F., Balebako, R., Durity, A. L., & Cranor, L. F. (2015). A Design Space for Effective Privacy Notices. *Symposium on Usable Privacy and Security (SOUPS)*, (pp. 1-17). Ottawa.
Schlegel, R., Kapadia, A., & Lee, A. J. (2011). Eyeing Your Exposure: Quantifying and Controlling Information Sharing for Improved Privacy. *Proceedings of the Seventh Symposium on Usable Privacy and Security* (p. 14). ACM.
Shiffmann, H. R. (2001). *Sensation and perception: An integrated approach.* New York, NY: Wiley.
Shneiderman, B. (2000). Designing trust into online experiences. *Communications of the ACM, 43(12)*, 57-59.
Shneiderman, B., & Plaisant, C. (2004). *Designing the user interface: Strategies for effective Human-Computer Interaction.* Boston, MA: Addison Wesley.
Smith, A. (2003). A process model for developing usable web-sites. *Interacting with Computers, Elsevier*.
Tomitsch, M. T. (2008). Real-world tagging in the wild: On the usability and accessibility of NFC-based interactions. *In Workshop on Future Mobile Experiences: Next Generation Mobile Interaction*

and Contextualization, Co-Located with the Nordic Conference on Human-Computer Interaction, NordiCHI.

Union, E. (2016). Regulation 2016/679 of the European parliament and the Council of the European Union. *Off. J. Eur. Communities*, pp. 1-88.

Wagner, I., He, Y., Rosenberg, D., & Janicke, H. (2016). User interface design for privacy awareness in eHealth technologies. *Consumer Communications & Networking Conference (CCNC)* (pp. 38-43). IEEE.

van den Hoven, J., Blaauw, M., Pieters, W., & Warnier, M. (2016). Privacy and Information Technology. In E. N. Zalta, *The Stanford Encyclopedia of Philosophy.*

Xu, H., Wang, N., & Grossklags, J. (2012). *Privacy by redesign: Alleviating privacy concerns for third-party apps.*