D4.4

Social Requirement Analysis – v2

V1.3 / 2015-09-24

Tom Seymoens (iMinds), Laurence Claeys (iMinds), Jo Pierson (iMinds)

This deliverable describes the need for transparency enhancing technologies from a contextual privacy perspective. It shortly describes the two main theoretical perspectives in this field: Communication Privacy Management and Contextual Integrity. To underscore the urgency for more transparency, we compare user studies that were performed as part of USEMP with the insights we gathered from our literature study. We then take a closer look at the social requirements that were described in D4.1 and analyse their current implementation in the DataBait tool. Through the means of qualitative interview sessions with end-users, we want to stimulate a discussion towards an updated set of social requirements.

Project acronym	USEMP
Full title	User Empowerment for Enhanced Online Presence Management
Grant agreement number	611596
Funding scheme	Specific Targeted Research Project (STREP)
Work program topic	Objective ICT-2013.1.7 Future Internet Research Experimentation
Project start date	2013-10-01
Project Duration	36 months

Workpackage	WP4
Deliverable lead org.	iMinds
Deliverable type	Report
Authors	Tom Seymoens (iMinds)
Reviewers	Katja De Vries (iCIS)
	Andreas Drakos (Velti)
Version	1.0
Status	Draft | PMB Final Draft | **Final**
Dissemination level	**PU: Public**, PP: Restricted Program; RE: Restricted Group; CO: Confidential
Due date	2015-09-30
Delivery date	2015-10-09

Version	**Changes**
V1.0	Structure and introduction
V1.2	Literature review

V1.3	Methodology and results + update introduction and discussion
V1.4	Revision

Table of Contents

1.Introduction

Work package 4 aims to enhance our understanding of how users make use of Online Social Networks in their day to day life in light of the creation of a Transparency-Enhancing Technology (or TET): DataBait. Transparency-Enhancing Technologies aim to diminish the information asymmetry between data subjects and data controllers. An asymmetry brought up by the ambiguity of which data is collected and which data can be inferred. (Zimmermann, 2015) TETs are defined by Hildebrandt et al. (2006, p.107) as follows:

> "[…] Their function is not the history management of the data of a data subject, but the anticipation of profiles that may be applied to this a particular data subject. This concerns personalised profiles as well as distributive or non-distributive group profiles, possibly constructed out of anonymous data. The point would be to have some idea of the selection mechanisms (application of profiles) that may be applied, allowing a person adequate anticipation."

In a previous deliverable (D4.1) of this USEMP project, we distinguished 11 social requirements by means of four focus group sessions and a survey, send out in both Sweden by LTU and Belgium by iMinds. The aim of these social requirements was to gather some guidelines of what users understood under a tool that would help them enhance their privacy. In the current deliverable we try to build upon these requirements to guide the development process in the last year of the project.

We start the deliverable with a literature overview of how social platforms are becoming increasingly important in today's society and the effect this has on the privacy of its user group. Later on we take a look at privacy from a contextual perspective, investigating the theoretical frameworks of Nissenbaum (Contextual Integrity) and of Petronio (Communication Privacy Theory). The result from this literature review is that in order to create a more empowered social platform user, we believe a TET must give correct information about her complete audience and what information could be inferred about her. A user only has the chance to effectively manage her privacy when they have access to this kind of information.

In the second part of the deliverable we discuss the current (pre-pilot, August 2015) version of the DataBait tool and analyse how our social requirements are implemented into the system. We start with a short overview of the back end of the system (USEMP privacy scoring model) to see if we can already find traces of last year's social requirements implementation in this conceptual model. Later on, we present the results of 10 interview sessions in which we discussed the DataBait GUI with users to see if they felt the tool we are developing can help in privacy management tasks. We also analyse if the social requirements are included and present some new recommendations for updating and improving the system in the last year of the project.

Finally we will take a first look at some of the alternative visualisations proposed by CEA together with some users to see how we can enhance the usability. The results are some exploratory remarks that recurred during some of the interviews. This needs to be included in the pilot sessions.

2. Literature Study

2.1. Introduction: A Datafied World

Roughly in the last fifteen years, people have moved more and more of their social, cultural and professional activities to online environments. Their lives became permeated with social platforms which, according to José van Dijck (2013), had a great effect on the experience of sociality. As often happens when an innovation enters the market, and as underwritten by Gartner's Hype Cycle (Campani and Vaglio, 2015; Linden and Fenn 2003), the rise of social platforms was initially met with hype and inflated expectations. It was identified as the trigger to unlock the Internet's full potential as a place for nurturing connections, building communities and even advancing democracy, but the information companies that provide the means and structures enabling this transition to online environments are not necessarily adepts of these idealistic views. Their interest rather lies in the data, which is delivered as a by-product of maintaining connections online. These connections do not only connect people, but also persons to objects, brands etc. (Van Dijck, 2013). This transformation is made feasible by the rollout of technological force that enables the collection, storage and analysis of ever-increasing amounts of personal user data. The datafication allows information to be searched, combined and analysed at lower costs and without much effort (Pötzsch, 2009).

Some of the scholarly literature concerning datafication, makes a distinction between volunteered, observed and inferred personal information (See for instance WEF, Rethinking Personal Data: Strengthening Trust 2012). The first one can be defined as the type of information that a user consciously releases online. Observed information is typically the result of the transaction between a user and a website (where he clicks, from which location, how long he stays, etc.). Through the combination and analysis of volunteered and observed data, one can derive other information such as sexual and political preferences and psychological traits. This inferred data can be the outcome of what is being described by José van Dijck as *connectivity*:

> "[…] an automated process behind real-life connections that makes it possible to recognize people's preferences and desires. […] social media are inevitably automated systems that engineer and manipulate connections. In order to be able to recognize what people want and like, Facebook and other platforms track desires by coding relationships between people, things, and ideas into algorithms. (Van Dijck, 2013, p.12)"

People are in this way revealing more information than they might be aware of. Moreover, connectivity is an invisible process, carefully kept hidden from the social platform users as it is being branded as human connectedness. A very interesting analogy is being made by Heyman & Pierson (2014, under revision) where they link Facebook to Feenberg's concept of the "Colonisation of Lifeworld", as they note that:

> "[…] affordances on Facebook limit users' communication to those aspects that drive profit and connectivity. These evolutions pass under the radar because incremental updates further obfuscate critique of previous updates as the latter appear fixed due to the new update. (Heyman and Pierson, 2014, p.2)

A second, and connected consequence is that messages can reach an audience both unintended and unidentified, by the effortlessness data is being preserved over different locations and different times, e.g. when releasing information on social platforms, the user might consider his audience of peers, but it is unclear who else has access (e.g. partners of the data controllers, such as data brokers, advertising agencies, etc.). As such social platform users do not only reveal more information than initially intended, they might also share it with actors for which they consciously would retain types of information. Both institutional and social privacy violations (for a definition of social and institutional privacy, please see D4.1) might result from the uncertainty in which these users currently release their information.

We will examine privacy from a contextual perspective in the following paragraphs to understand better what is needed for effective privacy management in todays' datafied world.

2.2. Privacy: A Contextual Perspective

When looking at privacy from a contextual perspective, we acknowledge and embrace the fact that privacy in the current datafied world extends further than the mere control and access restriction by the individual (De Wolf, 2015). Privacy management is a social practice, where every actor needs to take context and different norms into account. This is particularly relevant as the Internet has made it much easier to share and reuse information that was shared under one intention and circumstance in other contexts. A short overview of the relevant literature (that is, the theoretical framework of contextual integrity and communication privacy management) is presented in the paragraphs below to better comprehend what needs to be provided to help the contemporary social platform user manage their privacy.

2.2.1. Contextual Integrity and CPM

As we witness the continuous move of social activities to online environments, which makes it easier to gather, store, analyse and manipulate social relationships and personal information, we need a framework that helps us recognize different privacy expectations present in this changing climate. For this reason, we choose to apply Helen Nissenbaum's (2004) "contextual integrity" framework. Barth et al. (2006) explain contextual integrity as follows:

> "It is not proposed as a full definition of privacy, but as a normative model, or framework, for evaluating the flow of information between agents (individuals and other entities), with a particular emphasis on explaining why certain patterns of flow provoke public outcry in the name of privacy (and why some do not)" (Barth et al. 2006, p2).

As the name of the framework already suggests, it's an approach to privacy that takes into account the specifics of the situation of action. The importance of context is underwritten by the notion that people's roles as they move around from situation to situation shift under the influence of the change of context. Two examples of everyday life clarify this: In the marketplace a person's role might be that of a consumer, while at his job he can be forced to act as an employer. Most of the contexts in which we act in our social lives have been developing for a long time together with a set of behaviour-guiding norms that prescribe how we operate in the given context (Barth et al. 2006). Nissenbaum (2004) mentions the following:

> "A central tenet of contextual integrity is that there are no arenas of life not governed by norms of information flow, no information or spheres of life for which "anything goes." Almost everything—things that we do, events that occur, transactions that take place—happens in a context not only of place but of politics, convention, and cultural expectation." (Nissenbaum 2004, p119)

In every transaction three entities can be distinguished: the sender, i.e. the one from who the information flows; the recipient, i.e. the one to whom the information flows; and the information subject, i.e. about who the information is (Barth et al. 2006). To preserve the integrity of a context, the sender cannot always freely transfer information about the information subject that was given in a specific context to another context or recipient. The norms that guide the process can be very explicit and specific, e.g. like the highly ritualized

norms guiding behavior within the setting of a church, whilst in other contexts they can be implicit, variable or (partially) incomplete (Nissenbaum 2004, p119).

Two main informational norms are differentiated in the literature: norms of appropriateness and norms of distribution (or flow). Norms of appropriateness define the type of information that may be released in a given situation, taking into account such principles as confidentiality, reciprocity, control and others. An elucidating example is the following: When a patient walks into a physician's office it is relevant and fitting that the physician asks the patient to reveal health information and symptoms he may have, so a right judgment can be made. It would however not be appropriate if the patient requests the same information of the physician or if a stranger asks a person these questions on the street. The second kind of informational norms are termed norms of distribution (or flow). These handle rules about to which contexts and recipients certain information may move. Let's take another look at the example of the physician-patient relationship. It would not be correct if a physician talks about the patient's medical condition with some of his friends, but it could be appropriate that he talks to a colleague about the symptoms to come up with a better treatment. Personal information revealed in a particular context is always tagged with that context and never "up for grabs" (Nissenbaum, 2004). If one of the two, or both informational norms are violated a privacy breach has occurred.

If we apply this framework to the social platforms in which we currently perform a great deal of our transactions, we see that privacy breaches can easily happen when users are not fully aware about the automated processes behind online sociality, described by José van Dijck (2013) as automated connectivity. If users make choices about what they voluntarily upload online, but are not aware of what else could be inferred based on their uploads and behavior a violation in the norms of appropriateness can occur. The norms of distribution are also under pressure in such a culture of connectivity, e.g. when users post information on a certain social platform thinking of one audience (e.g. their friends) but are not aware of the data mining algorithms, tracking cookies and data brokers that track their behaviour and through which the information also gets transferred to different contexts. Such a privacy violation is especially exhibited when users consciously want to differentiate in access rights towards different audiences. In this example the perceived context of the user is much smaller than the complete actual audience (Pierson and Heyman 2011).

Both given examples result in a privacy violation. The problem is clearly stated by Brunton and Nissenbaum (2011):

> "The lack of capacity to assess consequences in full is deeply troubling. We do not know all that they know about us, how they come to know it, or even who all the significant players might be. We cannot easily subject them to symmetrical analysis: such organizations might operate under the veil of national security or proprietary trade secrets, and we likely would not have the methods or the training to do anything with their data if we could get our hands on it. As people whose data is being collected, what we know of the situation is problematic, and what we do not know is substantial." (Brunton and Nissenbaum 2011)

Sandra Petronio has provided the research community with another framework for privacy assessment, called the "Communication Privacy Management Theory". Central to this theory is the claim that effective individual privacy management is an illusion. De Wolf (2015, p.33) words this as follows: Once private information is revealed, the receivers become co-owners of this information.

> "In order to preserve the privacy, mutually agreed upon privacy rules are needed and must be negotiated. When people fail to coordinate privacy rules, privacy turbulence occurs (i.e. embarrassing and/or problematic situations)" (De Wolf, 2015, p.33).

"Communication Privacy Management Theory" sees the ability to do a cost/benefit analysis as one of the guiding mechanisms for effective privacy management. While the benefits of social platforms are clearly advertised (amongst others: the branded human connectedness, building and maintaining social relationships, convenience and personalized services), the costs are (made) more or less unclear to the average social platform user.

This is underwritten by a research published by Turow, Hennessy, and Draper (2015) where they found that a majority of American citizens don't have the correct knowledge to make informed cost-benefit choices about the way marketers use their information.

We need to take both useful frameworks into account when developing tools to effectively manage privacy.

2.3. User Empowerment in a Datafied World

The very nature of social platforms holds some disempowering aspects. José van Dijck sees social media as "[…] automated systems that engineer and manipulate connections. In order to be able to recognize what people want and like, Facebook and other platforms track desires by coding relationships between people, things, and ideas into algorithms" (Van Dijck, 2013, p12). The technological structures enabling and mediating online sociality often stay invisible and unchallengeable for the general public. When talking about disempowerment through the mediation of sociality, Pierson (2012) talks about 'issues of privacy', which concern problems that occur due to a lack of awareness towards the changing privacy and surveillance aspects. Here the user does not fully perceive how their digital activities are being monitored, processed, analysed and commodified by third parties (Pierson, 2012, p104). Self-expression and maintaining social relations online are endorsed by the information companies, because their commodification is becoming a lucrative business (Pierson and Heyman, 2011).

If we reconsider the contextual integrity framework of Helen Nissenbaum as explicated in the previous chapter, it seems that people reveal personal information on social platforms with a certain context in mind. If people acted in a logical system where the agents are fully aware of their context and in control of the flow of information, they would have full control over their privacy (Barth et al. (2006); Pierson and Heyman (2011, p.4)). Pierson and Heyman (2011) have shown in their research that the perceived context differs from the actual, complete context in which people act on online platforms (See Figure 1). As such, they define user empowerment as

> "[…] the degree of overlap between these two contexts, the bigger the overlap, the more empowered a user is to at least evaluate whether he or she should disclose PII in this context while taking privacy into account." (Pierson and Heyman, 2011, p.4)

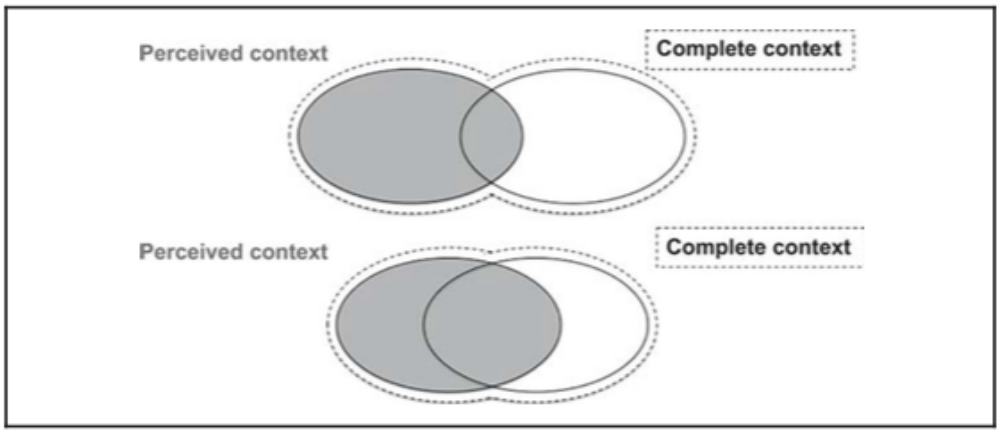


Figure 1: Perceived and complete context (Pierson & Heyman, 2011)

Not only should insights be provided about the complete contexts in which information is revealed. Users should also be fully aware of what information can be technically be inferred from their online behavior. In an interesting report, released by Turow, Hennessy, and Draper (2015) "The Tradeoff Fallacy" they indicated that American consumers are concerned about

how their data is being used and that they don't believe they get real insights into this process.

> "Although some online firms have been allowing Americans to see some of the data points they hold about them, the particulars of how and when they use these profiles – and with what other sources of information – is a mystery in almost all cases." (Turow, Hennessy, and Draper, 2015, p.19)

One of their main conclusions of their research project is very concise and interesting for our research, as they suggest a need to:

> "[…] advocate for the right to know one's profile and how it is used. As long as the algorithms companies implement to analyze and predict the future behaviors of individuals are hidden from public view, the potential for unwanted marketer exploitation of individuals' data remains high. We therefore ought to consider it an individual's right to access the profiles and scores companies use to create every personalized message and discount the individual receives. Companies will push back that giving out this information will expose trade secrets. We argue there are ways to carry this out while keeping their trade secrets intact. Without access to this information, individuals will continue to feel disempowered and disrespected by companies." (Turow, Hennessy, and Draper, 2015, p.21–22)

If users are unaware of the context in which they reveal their information, which processes underlie their online sociality and what information they reveal it is incredibly difficult to manage their privacy in a successful way.

2.4. Syntheses and Research Questions

Although it may seem that the only way users can preserve control over their data, is to stay offline, Privacy-Enhancing (PETs) and Transparency-Enhancing Technologies are at hand that help users to mitigate the risks. But in their current form they cannot be considered a success from an end-user perspective (Danezis et al., 2014). Privacy engineering is too often equated to the mere modelling and assessing of privacy risks and vulnerabilities in order to define and implement the correct remedies. The problem is the gap that exists between the abstract guidelines or assessment frameworks and the development process of the system itself. (National Institute of Standards and Technology (NIST), 2014)

Optimally, both the legal framework but also the end-user perception of privacy should be assessed within their framework of action and against the backdrop of possibilities for end-user control: which actions can the user take to enforce her rights and impact which information is disclosed. As such, there is a strong focus on the agency of the user, all the more because privacy concerns and risks can't be seen as a static characteristic. Hereby the context of use and the diversity that exists between users on the notion of privacy can be taken into account. This insight endorses the need for users to have a direct influence on privacy design decisions. Therefore, we have set up a collaborative procedural work between engineers, lawyers and social scientists from the start of the system definition process. In this way we aim to overcome the pitfalls that might have retained other existing privacy enhancing technologies to have an added value.

The theoretical literature review, which we presented in chapter, two of the current deliverable, shows the necessity to provide users with more transparency towards the operational and economic logic of social platforms. In order to make a correct cost – benefit analysis before revealing personal information, users need to be granted access towards the mechanisms underlying their sociality, that is, which inferences can be inferred from their digital trail and what the complete audience is of their online activities. In the following chapters we will see how parts of these recommendations are already integrated in the DataBait system and what could be adapted.

In the next chapters of this deliverable, we will take a first look on how the results of a first iteration of our social study was translated in the specifications of the DataBait system, both back and front end. Furthermore, our usability study with 10 users included discussing the different features already implemented and investigated how the participants rated them in relation to effective privacy management.

3.Social Requirements – Reprise

Social requirements stem from the examination of how users apply technologies in their daily lives and the needs that are subsequently created. In a previous deliverable of the USEMP project (D4.1), we distinguished a list of 11 social requirements that surfaced after conducting a survey (n=101) and four focusgroup sessions with 21 respondents. In short we could distinguish four groups of social requirements that a Transparency-Enhancing Technology (TET) should take into account. The first group talks about how a TET should deal with problems of awareness towards who collects data and what data can be gathered from the Internet. The second group talks about the incorporation of existing privacy strategies, such as reviewing pictures, incognito mode etc. Thirdly, we distinguished a group that talks about the necessity of more transparency online towards social platforms' economical logic, profiling tactics and which companies to trust. Finally we also separated a group that warns about some of the barriers that inhibit a widespread use of TETs such as bad browsing behaviour, but also that some control taking measures should be implemented. Table 1 shows an overview of all eleven social requirements. More information can be found in deliverable 4.1 of the USEMP project.

List of social requirements for the USEMP tools	
Group 1: Dealing with awareness	1. Linking online behaviour to known examples from the past of institutional privacy issues for raising awareness towards potential future institutional consequences.
	2. Presenting the user with tangible situations where user data was used for explicitly customizing a service (e.g. tailored advertising).
	3. Visualizing the several data brokers and partners to which they send their data.
Group 2: Existing strategies	4. Supporting existing privacy strategies by taking away barriers that inhibit a widespread use.
Group 3: Dealing with transparency	5. Giving more transparency towards the economical logic behind connectivity on the Internet.
	6. Handing over the necessary information by which the users can make an informed decision for trusting several online services and websites.
	7. The USEMP tools should take into account the diversity under its users related to trust-seeking behaviour.
	8. The trustworthiness of the organization behind the USEMP tools should be proven to augment the adoption capacity.
Group 4: Tackling the barriers	9. The USEMP tools should hold a clear value to the users, apart from privacy enhancement.
	10. Countering the bad reputation some web-browser plugins seem to hold by promoting its use through local experts.
	11. Incorporating features that do not only make the user more aware but by which he can also change his behaviour. This may imply that, as he gains more control, the attitude towards a TET-tool can become more positive.

Table 1: Initial list of Social Requirements for the USEMP tools

In the next sections we will take a look at how they are implemented in the system. It's not our goal to implement all of them, but we want to explore if they need an update or if we could ameliorate the output.

3.1. Back end of the system: implementation of social requirements in the USEMP Privacy Scoring Model

In this section we will take a closer look on how the social requirements are implemented in the proposed privacy-enhancing tool, Databait, more specifically into the underlying USEMP Privacy Scoring Model. More information on how this model was created can be found in (Petkos et al., 2015) and (Rizos, Papadopoulos, and Kompatsiaris, 2015).

This model is a tool that aims at raising the awareness of users about the disclosure and value of their personal information by giving disclosure scores to categories of personal data. As such providing users with more insights on data inferences and raising profile transparency. The model is based on eight privacy dimensions: demographics, psychological traits, sexual profile, political attitude, religious beliefs, health factors & condition, location and consumer profile. Each dimension entails a set of attributes that were chosen because people consider them sensitive, they are considered sensitive from a legal perspective or they hold a value for marketing companies to target consumers. For the dimension of 'Health Factor and Condition' these attributes include amongst others habits (e.g. smoking, drinking), medical conditions, disabilities and health factors (such as exercising behaviour). Here it is already clear that social research and legal research have a direct influence on the back end of the system by helping with the development of the list of attributes through our collaborative approach. The dimensions and attributes are not exhaustive and can change over time, to support changes in what might be perceived sensitive or private information.

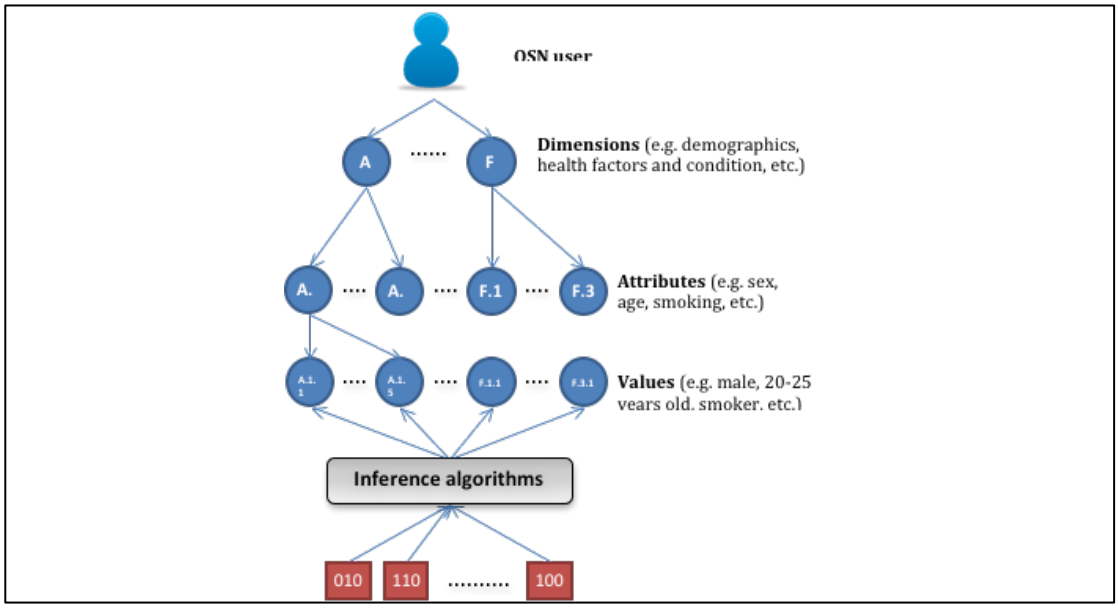


Figure 2: USEMP Privacy Scoring Framework (Ref. Popescu et al., 2015)

Figure 2 provides an overview of the privacy-scoring framework and how it is built up out of dimensions, attributes and values. At each level of the framework privacy scores are attached: a higher score denotes a higher privacy exposure for the given attribute and dimension. The privacy scores are made up of:

- Sensitivity scores (how sensitive a user finds a piece of information, self-acclaimed or based on a-priori score of the average user, based on our USEMP user study)
- Visibility scores (the size of the audience of the piece of information)
- Confidence score (if the user has exposed the piece of information itself, the confidence score is 1, if it is computed based on inference mechanisms it can vary between 0 and 1)

To better understand how the privacy-scoring framework works, we take a look at an example. Imagine a user making use of the DataBait plugin, who goes to take a look at his privacy profile of an online social platform. He then for instance sees that the dimension of 'Health Factors & Condition' has a high disclosure score. Interested in what causes this, he clicks through to the underlying level of attributes. Here, he sees a high score for smoking. Subsequently at the value level he sees that he apparently has released some information on the Internet that gives away that he is a smoker. This can surprise him, as he does not understand what caused this inference. He can then click through and get a view on the exact pieces of information that have caused the inference mechanisms to categorize him as a smoker, for instance a picture of the user holding a cigarette. He doesn't only receive insights on his privacy scores, but he can influence it as well, for example by stating that he does not find it sensitive that he discloses that he is a smoker.

The privacy-scoring framework allows a user to get more awareness towards which pieces of information he reveals and how this is used (**first group of social requirements**), he can also actively act on this, not only in the tool but also by changing his behaviour elsewhere (**which is linked to the last group of social requirements**). As proposed in our theoretical part about user empowerment the raising of awareness can help the user to get more empowered towards the risks of his information disclosure.

The privacy-scoring framework is in part speculative: it does not say that this information is actually inferred or used by commercial actors tracking the user. It only shows him what *could* be inferred and what is technically possible. Sometimes, wrong inferences might be made (e.g. a blurry picture with no cigarette in it, could be a reason to be misclassified). This might enlighten the user to see how the existing algorithms still have some flaws, or how he can also be wrongfully targeted online. It's about generating the right amount of transparency towards the end users (**third group of social requirements**). Instead of doing this by granting access to the actual algorithms as proposed by Turow et al. (2015) (see paragraph 2.3 of this deliverable), it provides this transparency by granting insight into the technical possibilities.

3.2. Front end of the system: implementation of social requirements in the DataBait GUI

3.2.1. Overview

In the following section we will investigate how the social requirements are implemented in the DataBait Graphic User Interface (GUI). This section is the result of a desk study where we compared the social requirements with the current version of the DataBait tool, as well as 10 different in-depth interview sessions. Through these interviews we wanted to explore if the features presented help give users more transparency and control and if they thought some other features were missing. We preferred the use of individual interviews over group sessions because we wanted to understand each users' motivation to accept or dismiss a functionality.

3.2.2. Design of the interviews

10 interview sessions were conducted in Dutch throughout the first two weeks of September 2015. We opted for a population of mixed gender and age. The only necessity was that the participants had an account on the social platform Facebook. To recruit respondents, we relied on the expertise of iMinds' living labs. We made use of a selection of people who also participated in the pre-pre-pilot of the USEMP project, because they already had a working DataBait account and in this way we could circumvent spending too much time on the extensive registration process. Our aim was to reach at least 10 respondents. As an incentive, we provided the user with a voucher of €25 for a Belgian retail chain for books and multimedia (FNAC). Eventually 5 male and 5 female participants agreed to partake in the interviews, their ages varied between 20 and 53. The interviews lasted on average 1 hour and 30 minutes and took place at the respondents' home, the iMinds offices in Ghent or the iMinds offices in Brussels. All sessions were tape-recorded. To ensure anonymity, all respondents received pseudonyms in the transcriptions, which will also be used in this deliverable. Table 2 summarizes the participants' demographics and timing of interviews.

Interview	Date	Name (gender)	Age	Professional Situation	Frequency Facebook use
1	04/09/2015	Neil (m)	37	Employed	Several times a day
2	07/09/2015	Kathy (f)	45	Unspecified	Several times a day
3	07/09/2015	Nina (m)	27	Employed	Weekly
4	07/09/2015	Courtney (f)	38	Employed	Several times a day
5	08/09/2015	Paul (m)	32	Employed	Daily
6	09/09/2015	Bob (m)	20	Student	Several times a day
7	09/09/2015	Joni (f)	23	Employed	Several times a day

8	13/09/2015	Sylvie (f)	24	Employed	Weekly
8	17/09/2015	Rick (m)	53	Employed	Weekly
10	18/09/2015	Tim (m)	28	Employed	Several times a day

Table 2: Overview of the participants' demographics

To leave sufficient room for discussion, we opted for semi-structured interviews. A script was prepared, mentioning the major topics and some key questions we could use in order to spark the discussion. The interview sessions were structured as follows:

1. Short introduction, explaining the voice recording of the session and the general outline of the interview sessions
2. Asking the respondents to fill in some questions about their privacy profile and general questions about online privacy
3. Testing the different implemented features of the DataBait tool
    a. login and registration process
    b. DataBait information page
    c. Image Leaks
    d. Location Leaks
    e. Trackers
    f. Audience Influence
4. Talk about missing features and extra requirements
5. Prototype of some new visualisations

The full script (in Dutch) can be found in the Annex at the end of this deliverable.

In the next chapter we will take a look at the different social requirements as they were defined in deliverable 4.1 and how they have been implemented into the front end of the system. For each group of social requirements we have performed first a desk study to see where and if we could see them represented in the tool, while later on added some comments of users regarding these features and if they could be improved in some way. As deliverable 4.1 described an overview of what *could* have an added value for new privacy enhancing tools, not all social requirements are to be found in the tool. Choices needed to be made in order to make the tool standout with a clearly defined value.

3.2.3. Report

A. 1st Group of Social Requirements: Dealing with Awareness

SR1:
The USEMP tools should make institutional privacy problems more tangible and understandable. Right now, institutional privacy problems are still perceived as future-oriented and not an everyday life problem. This could be done separate or as part of the USEMP tools, by **linking their online behaviour to known examples from the past of institutional privacy issues**.

Recommendation: This requirement is not present in the current version of the DataBait tool. Our second round of user studies still show a lack in comprehending the full scope of institutional privacy issues. Social privacy issues are still easier to grasp and come to mind much faster when probing our users about online privacy. Extra information should be given on how for example the way users define their online identities can have tangible outcomes, such as price discrimination.

SR2:
The USEMP tool should have the ability to generate tangible situations where user data was used for customizing a service (e.g. advertising, recommendations on Amazon). A possible way to do this is by **describing the possible data inputs that users created that may have led to the appearance of a specific advertisement and other tailored features.**

This requirement can be found in a specific way in the DataBait-tool. No advertisements have been used, the general idea was brought to a more abstract level as the DataBait tool holds the possibility to make the users more aware of which data points lead to which inferences. A clear example can be found in the 'Image Leaks' function of the tool. Here the user is presented with a tag cloud of concepts that were inferred from the user's images. When she clicks on one of the concepts she then gets insight into which data points (images in this case) have revealed them. (See figure 3). Also the location leaks function of the DataBait tool works in a similar way: the user gets presented with a cloud of locations, if she clicks on a location he sees which status updates (data points) have revealed her connection with the city and with what probability this can be inferred. Although the locations were not accurate, users seemed to like the idea of both functions.

Figure 3: Implementation of SR2

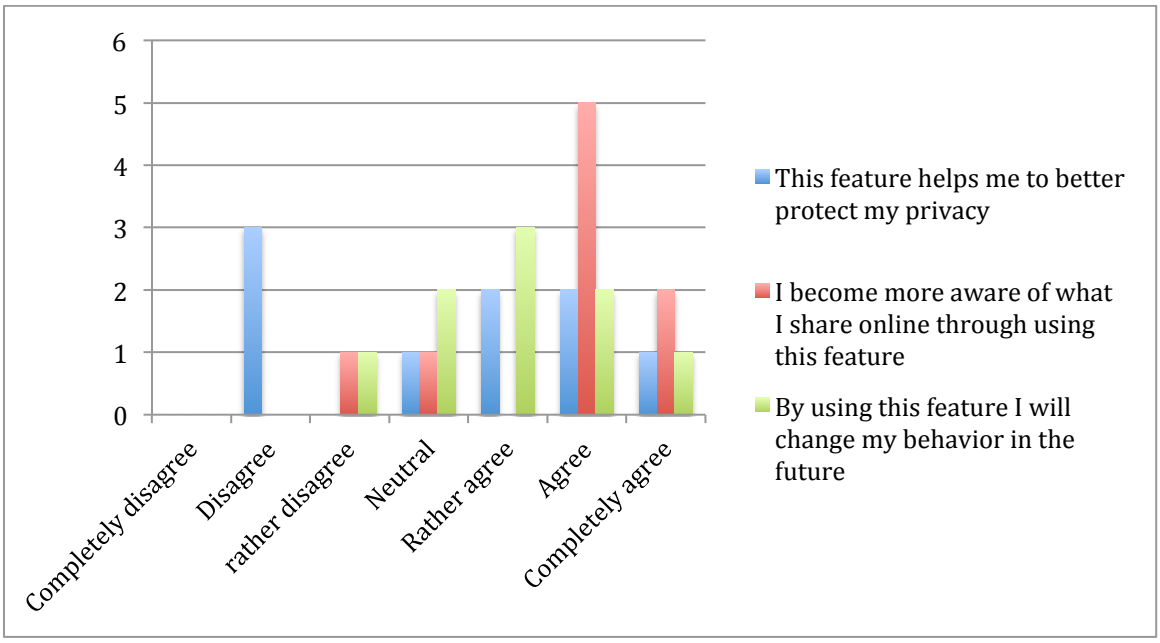


Figure 4: Image Leaks (n=9)

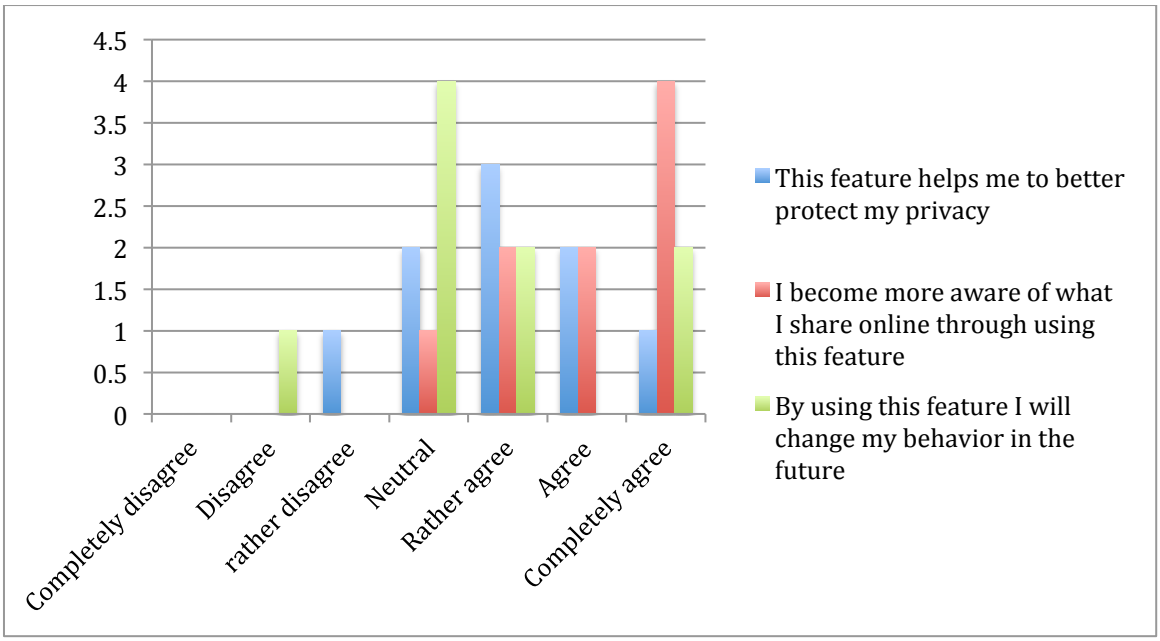


Figure 5: Location Leaks (n=9)

Recommendations:

- Currently the image leaks function shows a word cloud of all the concepts that could be attached to one of the pictures (out of a list of 17 000 concepts). This has as an effect that not all concepts showed contain sensitive information. Although some users did find it a nice alternative visualization of their pictures and it helps to understand how good current data mining techniques work, it would be better to group the concepts according to what type of information they reveal (link it with the privacy dimensions defined in WP6 for example). In this way the overview becomes much clearer. For example that a cat is depicted might not mean much to the user,

unless we link it immediately to the fact that this might reveal some of his consumer information. Users should also be given the opportunity to mark the information concepts they find privacy intrusive in the tool. We can learn from this, and it is beneficial for the user as well since he only gets to see the inferences about the concepts he finds relevant. The visualisations developed by CEA and presented in the next section are a step in the right direction.

- Figure 4 and figure 5, although made with a very limited population, reflect the interviews we had with the participants. We can see that the features help make users more aware about what they share, but that they don't necessarily feel it will help them protect their privacy.
- The location leaks function also helps to show which data points reveal which information. Especially when they concern status updates from the past this works as an eye opener for some respondents. An issue is that they are not very accurate. It would be great to also visualize the locations in a different way: to map them on a timetable as to show that it's possible to predict when a respondent is on which location.

SR3:

The USEMP tools should make users more aware of which types of organizations are collecting their data on the Internet and should be able **to visualize the several data brokers and the partners to which they send their data.**

This requirement can be found through the tracker function of the DataBait tool. When the user also installed the DataBait browser plugin, he gets an overview of which data brokers collect his information on different web pages that he visits. He can get it in real time by clicking on the plugin in the top left of the browser (for now only available for Google Chrome) (See figure 6). Later he can also visit the DataBait website to get an overview of all the webpages and corresponding trackers (See figure 7). Where possible, he can deny some of the trackers access to his information.

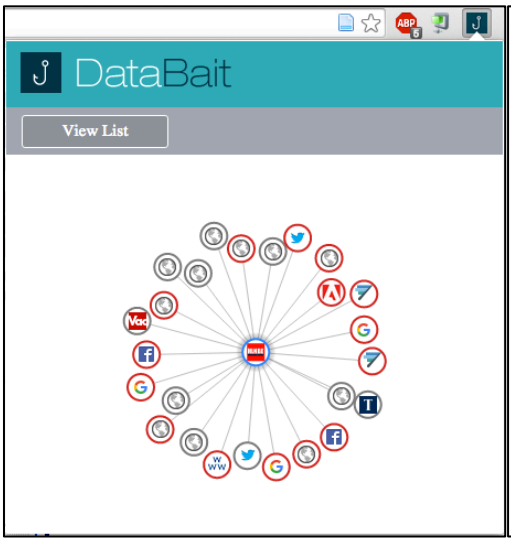


Figure 6: Implementation of SR3 (a)

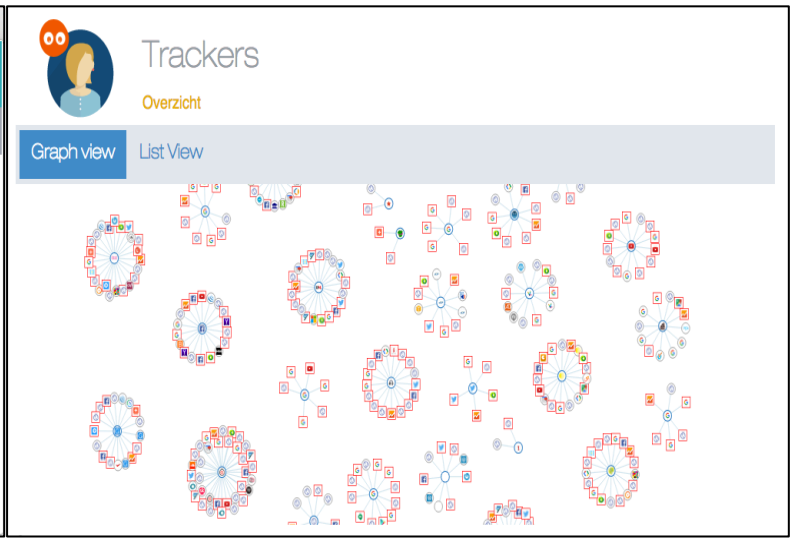


Figure 7: Implementation of SR3 (b)

Recommendations:

- Although a very nice feature that seems to work pretty well, we should also provide users with more transparency about the aim of such tracking companies. How do they use the information, who do they sell it to and what will be the results of this? This would help to understand the actual processes and could help users to decide for which companies they want to turn of the tracking. We should make it clear that some websites live from advertising and explain such a business model so users can make an informed choice.
- The plugin that was developed for this function to work is a nice added feature, especially because you can already see the visualization there. It would be nice to develop this further into a mini-dashboard, where the user can also easily be referred to the full website or get some other options related to tracking (like enable/disable all).

B. 2nd Group of Social Requirements: Learning from existing strategies

SR4:
The USEMP tools should **support the existing privacy strategies by taking away barriers that inhibit a widespread use**. It could do this by incorporating them inside the tools as possible alternative ways for users to be empowered. The tool could for example link to alternative search engines (such as DuckDuckGo), have a button for deleting cookies, switching to private browsing, reviewing pictures on Facebook etc.

This is not fully included in the current version of the DataBait tool. When we posed this feature to our respondents they did not fully agree that this should be implemented because it might overburden the tool.

The image leaks function can be seen as an alternative way of reviewing pictures on Facebook since they get linked with certain concepts. If the user then does not like that a certain concept can be inferred from her profile, it can help her to decide which pictures should be deleted.

Recommendations:

- Although not everyone is fully convinced that the tool should become a central hub with several features, we could easily include some features. This could be done in the browser plug-in. As a quick way to go delete cookies or do incognito browsing
- Alternatively, we could create a special page with links to other privacy enhancing technologies and how they work. Another feature might be a compilation of hands on guidelines of what users can do to protect their privacy better.

C. 3rd Group of Social Requirements: Dealing with the problems of transparency

SR5:
The USEMP tools should **give some more transparency towards the economical logic behind connectivity on the Internet**. This could be done by giving an estimation of the value of their personal data with a visualization how USEMP calculated this.

In the scope of USEMP we decided to leave this track and focus on transparency of profiling and data mining mechanisms instead.

SR6:
The USEMP tools should **help users in their negotiation of which websites to trust by handing them all the necessary information**. This could be done by handing the users a simple privacy rating of the websites they visit and linking to the central bullet points of the websites' privacy statement.
This is not included in the current version of the DataBait tools and probably not feasible to do for every website.

Recommendations:

- A handy feature could be to include a rating and some bullet points for some of the major websites that effect users with their privacy statements, e.g. Facebook, Google, Twitter, … We can then also link to other available initiatives such as tosdr.org where more websites are being rated.

SR7 and SR8:

- ❖ The USEMP tools should take into account the **different type of users related to trust-seeking behaviour**. One solution doesn't fit all
- ❖ The USEMP tools should understand that **the trustworthiness of the tools are connected with the organization launching the application**. The trustworthiness of the organization should be proven to augment the adoption capacity.

We took these two social requirements together, because they both refer to the trustworthiness and transparency of the organisations behind the DataBait tools. Many features have been implemented in the tools already to give the users more transparency: an easily readable contract, an explanatory video, a page with information about data mining, contact information and a page about which data is being processed. When questioning the participants during the interviews this seemed to be sufficient to get a trustworthy image. Although the users stated they would never read the contract or all the information pages, it was sufficient that they were there.

Recommendations:

In light of the Data Licensing Agreement, users stated that a catch phrase per clause of the contract was something that could help them understand the text better. They would not read the whole agreement, but it would be nice to get an overview of what is exactly in there by the visualization of some key words.

D. 4th Group of Social Requirements: Countering obstacles for using TETs

SR9:
The USEMP tools should have a **clear value, apart from privacy enhancement**, to the user. Different possibilities could be considered: gaming, monetization, social interactions.

This social requirement had the intention to create a larger audience for the tool by means of an added gadget value that would be tested and at the same time would educate about privacy issues. Although the emphasis is not on this in the current DataBait tool, all features that are currently implemented hold some kind of gadget value that creates interest among its users. Some of the users for which the tools failed to load their images reacted disappointed and were eager to learn which concepts could be attached to their pictures. The users were interested to see which concepts would be attached to their images and status updates. The audience influence function, in which the user can see which friends have interacted most with their content (based on likes) holds the greatest gadget value. Users claimed it did not help them much with privacy, but it was something nice to see visualised for once (see Figure 7).

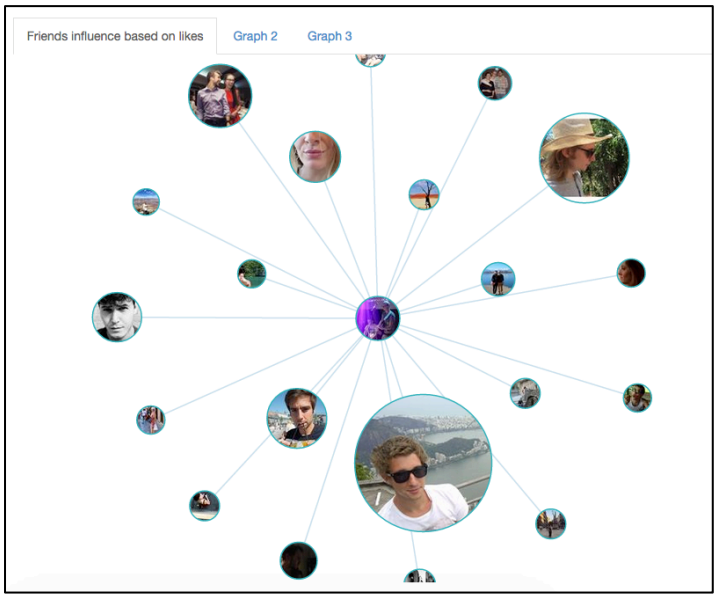


Figure 8: Audience Influence function

Recommendation:
We should not focus too much on finding additional reasons to make users download the tool. The features that are included suffice to get the interest of our population. It would be very patronising to 'trick' users to get interested in online privacy.

SR10:
The USEMP tools should **counter the bad reputation that web-browser plugins seem to have and they should be promoted more**. One way of doing this is by reaching local/warm experts that can persuade other users. More research needs to be done on how to reach these trusted opinion leaders.

If we make use of a web-browser plugin to show which trackers are available, we should make sure that it works fluently without slowing down the browser experience. The current browser plugin does not always work fluently, as some websites do not load as a result of this. Reaching out to local experts is still something we have to do for marketing purposes once we get closer to the end of the project and thus definitely in the upcoming year. It is very important to take this into account with the upcoming pilots.

SR11
A social requirement of the USEMP tools would be that it holds the necessary functionalities to be adequately informed and act on this information. In essence this would mean that **USEMP tools incorporate features that do not only make the user more aware but by which he can also change his behaviour. This may imply that, as he gains more control, the attitude towards a TET-tool can become more positive**.

A social requirement we still **have to take into account** in the last year of the project. As shown in the charts in figure 6 and 7, our respondents do not necessarily feel that their privacy will become more protected through the use of the DataBait tool, as it is still very much focused on transparency. But as we learned from the literature study, transparency towards who are collecting and processing data and what data can be inferred from which data points is already a first step towards a more effective privacy management as it helps the user to make a cost/benefit analysis based on correct information. Nevertheless, we don not want users to become resigned as is discussed in Turrow et al. (2015) where it seems that the most informed users get more resigned towards data collection for marketer purposes.

3.2.4. Visualisation Testing

If at the end of the interview sessions we still had some time, we decided to run over some of the high fidelity prototypes of privacy visualisations developed by the CEA research team. Please note that due to this reason, the population was very small and we will focus here on some of the main remarks that recurred. This needs to be tested further in follow-up interviews or as part of the pilot.

Three visualisations were tested as depicted in the pictures below:

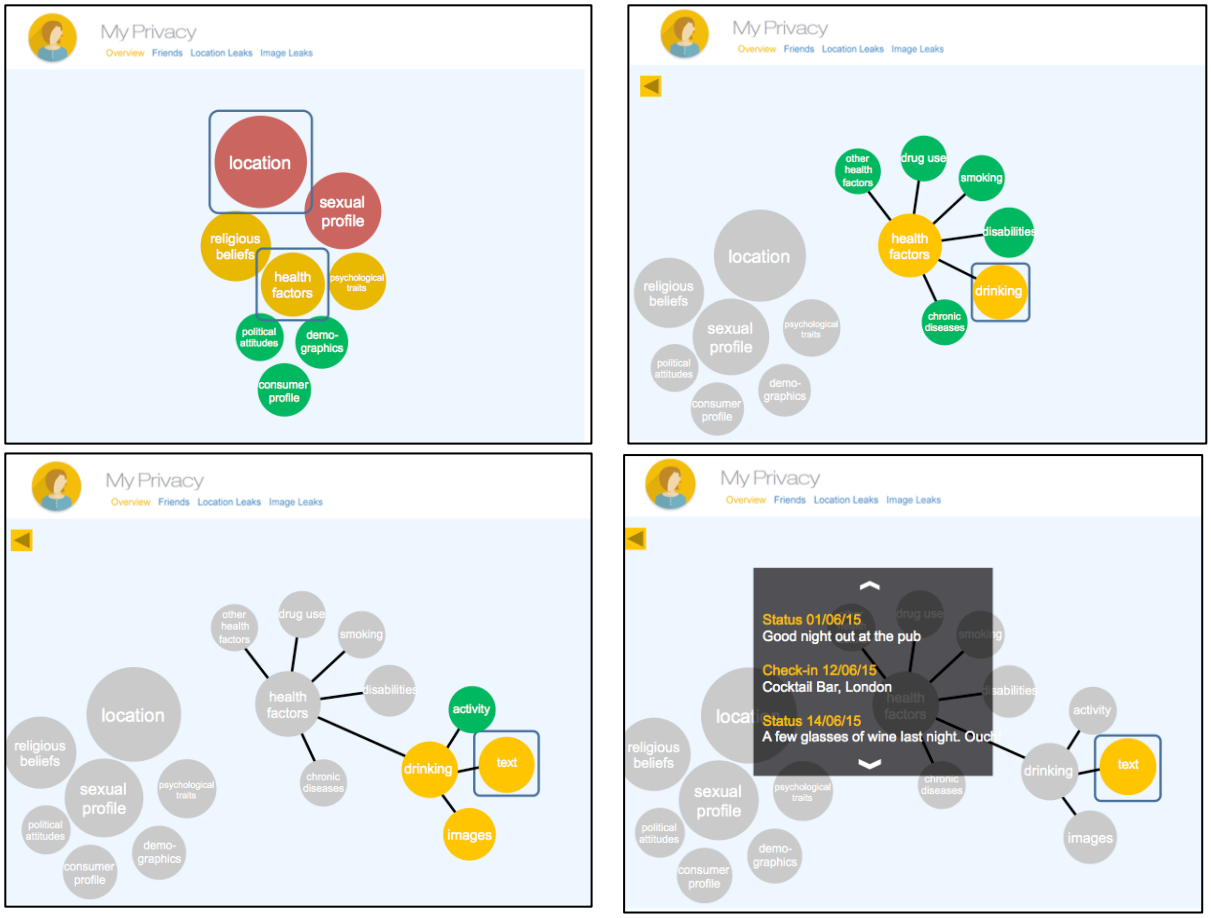


Figure 9: Visualisation Privacy Dimensions

In general, this visualisation was well received. It made it clear through which data point other information of the information subject could be inferred. A little bit of confusion existed about the first screen with our respondents. They did not immediately understand why the location bubble was coloured red and the biggest. Respondents assumed it was because this was the most sensitive information, which was not the case. The largest, red bubble means that the user revealed the most information about this subject. All in all, this would be a great visualisation alternative, because the user can immediately click through to the concepts he wants to learn about and doesn't have to search in a list of concepts. This can be linked to the recommendations given above when discussing the second social requirement.

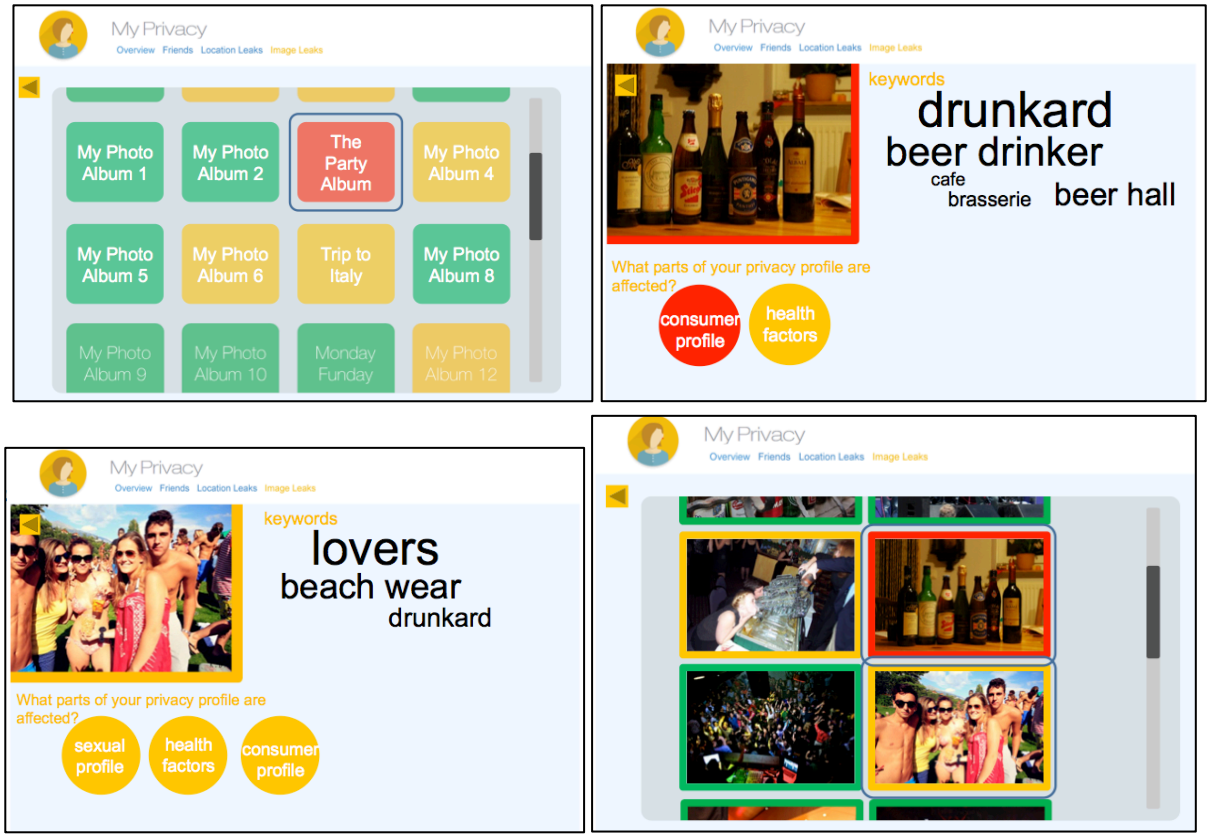
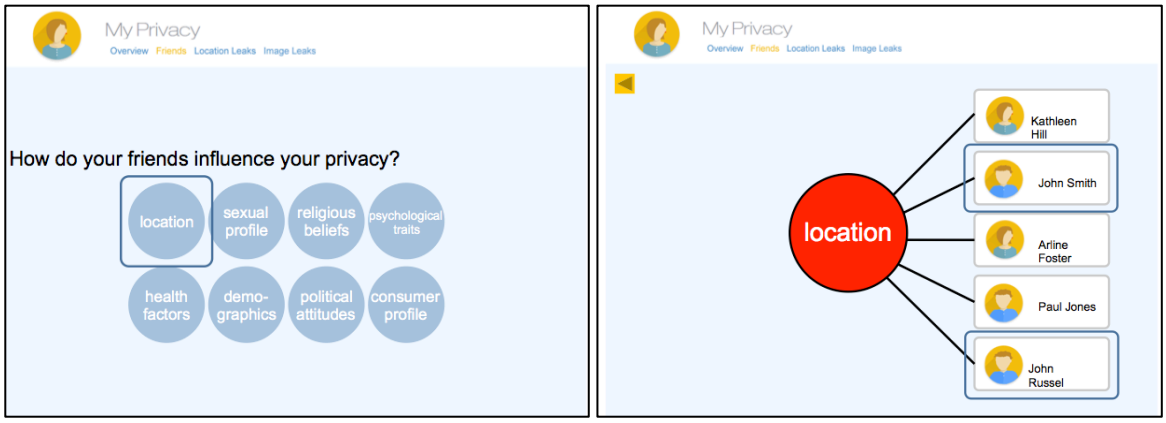


Figure 10: Visualisation photo albums

This visualisation was also found to be interesting by our respondents. Some mentioned that over the years they had gathered many photo albums on Facebook of which they forgot the existence or never really go back to. Through this visualization they claim they would see immediately where the potential privacy issues might be situated and could delete the whole album or specific pictures of the album. The general structure of this visualisation was easily understood.



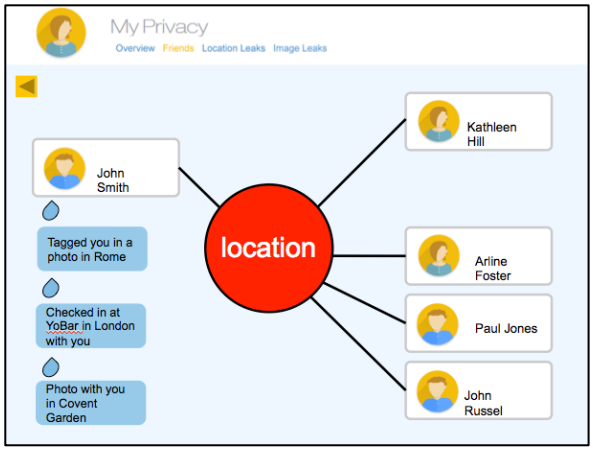


Figure 11: Visualisation Friends Influence

The last visualisation we discussed with our respondents was also a top down one, starting with an overview from the different privacy dimensions. This one was received with less enthusiasm than the previous two. This was mainly because users mentioned that they clearly knew which of their friends tagged them most in locations or pictures. If they did not agree with the tag they would immediately talk to them about it. They didn't see the added value of a visualisation that shows them who reveals most about them. Also most of our users used timeline review, a feature of Facebook that controls what appears on your timeline, and they mentioned that they felt it gave them sufficient control.

4. Conclusion and Next Steps

In the current world where social, cultural and professional activities are increasingly being moved to online environments (Van Dijck 2013), it is a challenge to support users with their privacy management tasks. In the USEMP project it's exactly this challenge that we try to counter by developing a privacy enhancing technology that warns the users about the risks and potentials of personal information sharing.

We started this deliverable by glancing over the relevant literature to understand where privacy violations might occur and how we can help to counter the threats. According to Nissenbaum's contextual integrity framework, a privacy breach occurs when the relevant partners do not abide by the norms of appropriateness and norms of distributions. In a datafied world it is currently very difficult to find out which information circulates about a person, how they are being profiled and what is the complete audience.

In a report by Turow et al. (2015) it is stated that users need to get more insights in the data mining mechanisms and the way in which profiling takes place to enhance the transparency. They see the need to get an overview of the actual algorithms that the social platforms apply.

Social platforms often do not reveal the actual algorithms they are using, and defend this by labelling them as trademark secrets. In the USEMP project we do not aim to uncover these algorithms, but use an alternative approach to provide the users with transparency. By means of the DataBait tools, we try to enhance transparency towards profiling by showing what data points make it *technically possible* to infer information, which the social platform users did not consciously reveal.

In this deliverable by means of a desk study and 10 qualitative interviews we distinguished a number of hands-on recommendations to update the social requirements that were created last year and bring the tool closer to what the users claim they need for a better privacy management.

Now we need to discuss these recommendations with the technical partners and implement the proposed changes, so we can test it in full in the upcoming pilot tests. In order to create added value we need to see how we can give the social platform users enough transparency. Next to this we also need to give them enough means for control so they do not get resigned in relation to their privacy management online.

5.Annex

5.1. Qualitative interviews – walkthrough

5.1.1. Inleiding + Usability Interview Agenda

- Korte inleiding + Introductie USEMP project + Informed consent
- Profileringsparameters
- Social Requirements
- DataBait tool
- Audience Influence
- Visualisaties Steven

5.1.2. Korte inleiding + introductie USEMP project + Informed consent

- Interview over wat jij verwacht van instrumenten die je helpen meer inzicht te krijgen in jouw online privacy
- Heel belangrijk dat je als respondent luidop praat, wat je denkt interesseert ons
- We zijn niet op zoek naar juiste of foute antwoorden, maar naar verschillende meningen over online privacy
- Het interview wordt opgenomen, maar zal enkel gebruikt worden om te transcriberen, alles wordt anoniem verwerkt en nooit zal een derde persoon dit gesprek horen.

5.1.3. Profileringsparameters

- Waarom neem je deel aan dit soort sessies? Ruim: hoe sta jij ten op zichtte van online privacy?
- Link Qualtrics: https://iminds.az1.qualtrics.com/SE/?SID=SV_38Xu7X0iN49TF8F

5.1.4. Inleidende vragen: Online privacy

- Hoe zie jij dat nieuwe technologieën een effect hebben op jouw privacy?
- Wanneer je een nieuwe technologie gaat gebruiken, hou je dan op voorhand rekening met de gevolgen voor jouw privacy? (Kosten/baten afweging, vb. Sociale Media, nieuwe gsm, Windows 10 update)
- Ben je op de hoogte van het bestaan van software, plug-ins, applicaties die je persoonlijke data helpen te beschermen?
    - Welke zijn bekend voor jou?
    - Heb je er al aan gedacht om zo'n tools te gebruiken? Gebruik je ze reeds? Waarom niet?/Waarom wel?
    - Wat is voor jou het belangrijkste zodat je zo'n tool zou gebruiken?
    - Wat zou je tegenhouden? Zie je er iets negatief aan?

5.1.5. DataBait testing: Inlog & Registratieproces

- 1st: Registratie proces (ook al hebben ze al een account, luidop laten praten over wat er gebeurd:

    - Ouder dan 13?
- DLA
    - Zie je een verschil tussen ons contract en de privacy statements/terms of service van andere online diensten?

Contract is bedoeld als duidelijker geformuleerd, korter, mutuele verbintenis worden uitgelegd,

        - Wat vind je hiervan?
    - Heb je dit contract tijdens je registratie bekeken? (grondig doorgenomen, oppervlakkig doorgenomen, zo snel mogelijk weg geklikt)
        - Wat is hier de reden voor?
    - Was de informatie duidelijk geformuleerd? Gemakkelijk te begrijpen?
- TERUG NAAR QUALTRICS
    - Het Contract
        - Was er nog andere informatie die je interessant vond?
        - Miste je iets? Waren er onduidelijkheden aan het contract?
    - Algemeen Registratieproces
        - Als er problemen waren? Welke waren dit dan?
    - Wat vond je ervan dat DataBait verbinding wou maken met jouw Facebook profiel?

5.1.6. DataBait Informatiepagina

Peilen naar DataBait: what, why and how?

- Eens ingelogd, waar zou je naartoe gaan om meer informatie over het DataBait project/tool te vinden?
- Vind je hier wat je zocht? Wat wens je hier meer te zien?
- Is er iets wat je stoort?
- Vind je de lay-out toegankelijk?
- Vind je dit meer overzichtelijk dan het contract dat je hiernet hebt bekeken? Heb je hier meer aan?
- Miste je hier informatie?
- TERUG NAAR QUALTRICS
- In hoeverre straalt de tool vertrouwen uit? Ga je ervan uit dat de ontwikkelaars van de tool te vertrouwen zijn? Is er voldoende transparantie? Mis je iets?

5.1.7. Image Leaks

- Wanneer gebruik jij Facebook? Voor welke reden gebruik je Facebook?
- Welke functies van Facebook gebruik jij het meest?
- Deel je veel foto's via Facebook? Wat voor foto's zijn dit dan? (Vakantiefoto's, feestjes, evenementen, …)
- Met wie deel je dan deze foto's? Hou je je bezig met wie allemaal kan meekijken wanneer je een foto post?
- Met welk apparaat gebruik je het meest om foto's op jouw Facebook te plaatsen?

- Zijn er situaties dat je je voor de geest kan halen dat je geen foto plaatst? Waarom? Wat is de reden dat je bepaalde foto's niet deelt
- Denk je dat er dingen uit jouw foto's afgeleid kunnen worden, die je liever geheim houdt?
- Nu je weet hoe de techniek hierachter werkt (data extraction/data mining) denk je dat het (in de toekomst) mogelijk wordt om meer private informatie af te leiden (zie wat de respondent tijdens q card bij meer problematisch heeft gelegd)

Ga terug naar: https://databait.hwcomms.com/

We hebben in de laatste updates van de DataBait tool een functie gemaakt, die je helpt om te bekijken wat er allemaal uit jouw foto's kan worden afgeleid of welke concepten hiermee verbonden worden.

Ga op zoek naar de functie waar je kan bekijken met welke concepten jouw foto's verbonden worden

- Is deze functie op een goede plaats gelokaliseerd? Vond je snel wat je zocht?
- Begrijp je meteen hoe deze functie werkt?
- Waar zou je naartoe grijpen wanneer je niet begrijpt hoe dit werkt/je meer informatie wenst? Hielp dit je om meer te begrijpen hoe alles in zijn werk gaat?
- Vind je dit een nuttige functie? Komt dit overeen met wat je verwacht had?
- Wat vond je er nuttig aan? Wat verwacht je nog meer van zo'n tool?
- Kreeg je hierdoor een bepaald inzicht? Zou dit gedragsaanpassingen bij jou teweegbrengen? Bepaalde functies die je nog meer verwacht van zo'n tool?
- Wat vind je van de weergave? (Font sizes, duidelijkheid overzicht)
- Kan je 3 dingen opnoemen die je hier handig aan vond?
- Kan je een aantal dingen opnoemen die je zou willen veranderen? Was er iets niet correct?

Ga terug naar Qualtrics

5.1.8. Location Leaks

- Deel jij gemakkelijk jouw locatie op Facebook? Wanneer doe je dit? Waarom?
- Vind je het een handige functie dat je andere mensen kan laten weten waar je bent?
- Denk je dat je jouw woon/werk/ of andere plaatsen waar je je bevind vrijgeeft via Facebook?
- Zijn er bepaalde plaatsen waarbij je zou overwegen om jouw locatie te delen?
- Zijn er bepaalde redenen waarom je dit niet zou doen? Of bepaalde situaties die je liever geheim zou houden?
- Hou je je bezig met wie allemaal meekijkt wanneer je je locatie plaatst?

Ga terug naar: https://databait.hwcomms.com/

We hebben in de laatste updates van de DataBait tool een functie gemaakt, die je helpt om te bekijken hoe jouw locaties afgeleid kunnen worden.

Ga op zoek naar de functie waar je kan bekijken met welke concepten jouw foto's verbonden worden

- Is deze functie op een goede plaats gelokaliseerd? Vond je snel wat je zocht?
- Begrijp je meteen hoe deze functie werkt?
- Waar zou je naartoe grijpen wanneer je niet begrijpt hoe dit werkt/je meer informatie wenst? Hielp dit je om meer te begrijpen hoe alles in zijn werk gaat?
- Was je je ervan bewust dat je deze informatie vrijgeeft?
- Vind je dit een nuttige functie? Komt dit overeen met wat je verwacht had?
- Wat vond je er nuttig aan? Wat verwacht je nog meer van zo'n tool?
- Kreeg je hierdoor een bepaald inzicht? Zou dit gedragsaanpassingen bij jou teweegbrengen? Bepaalde functies die je nog meer verwacht van zo'n tool?
- Wat vind je van de weergave? (Font sizes, duidelijkheid overzicht)
- Kan je 3 dingen opnoemen die je hier handig aan vond?
- Kan je een aantal dingen opnoemen die je zou willen veranderen? Was er iets niet correct?

Ga terug naar Qualtrics

5.1.9. Trackers

- Wie denk jij dat meekijkt wanneer je op het internet rondsurft? Aan welke bedrijven denk je dan vooral?

We hebben in de laatste updates van de DataBait tool een functie gemaakt, die je helpt om een beter overzicht te krijgen van welke bedrijven jou online volgen.

Ga op zoek naar de functie waar je dit kan bekijken.

- Is deze functie op een goede plaats gelokaliseerd? Vond je snel wat je zocht?
- Begrijp je meteen hoe deze functie werkt?
- Waar zou je naartoe grijpen wanneer je niet begrijpt hoe dit werkt/je meer informatie wenst? Hielp dit je om meer te begrijpen hoe alles in zijn werk gaat?
- Is dit een nuttige functie? Komt dit overeen met wat je ervan had verwacht?
- Wat vond je er nuttig aan? Wat verwacht je nog meer van zo'n tool?
- Was je hiervan bewust? Dat zo'n bedrijven je online volgen?
- Kreeg je hierdoor een bepaald inzicht? Ga je hierdoor in de toekomst jouw gedrag aanpassen?
- Wat vind je van de weergave?
- Is er iets wat je hier wenst aan te veranderen?

5.1.10. Audience Influence

Deze functie probeert de gebruiker inzicht te verwerven in wie van zijn vrienden in het verleden het meest met zijn data heeft geacteerd. Is een prototype functie. Werkt alleen met het account van de interviewer? (does it really?)

https://databaittest.hwcomms.com/welcome/audience/statisticaloverview

- Begrijp je meteen hoe deze functie werkt?

- Waar zou je naartoe grijpen wanneer je niet begrijpt hoe dit werkt/je meer informatie wenst? Hielp dit je om meer te begrijpen hoe alles in zijn werk gaat?
- Is dit een nuttige functie? Komt dit overeen met wat je ervan had verwacht?
- Wat vond je er nuttig aan? Wat verwacht je nog meer van zo'n tool?
- Kreeg je hierdoor een bepaald inzicht? Ga je hierdoor in de toekomst jouw gedrag aanpassen?
- Wat vind je van de weergave?
- Is er iets wat je hier wenst aan te veranderen?

GA TERUG NAAR QUALTRICS (afsluitende vragen usability, hele systeem)

5.1.11. Social Requirements

- Heb je het gevoel dat deze functies je meer bewust maken van wat je allemaal online deelt? Welke vind je tot nu toe de handigste?
- Sta je er van te kijken welke afleidingen kunnen gebeuren?
- Denk je dat je iets met al deze informatie kan aanvangen? Helpt je deze om je privacy te beschermen online? Voel je je meer in controle nu je dit weet? Of net niet
- Zijn er andere functies die je nog mist? Wat verwacht je nog van een privacy enhancing technology?
    - Andere privacy strategies toevoegen (incognito modus, settings sociale netwerk screenen, deleting cookies, informatie over websites (trust labels, privacy statements …)
    - Monetaire waarde (hoeveel geld je data waard is voor adverteerders)
    - Inschattingen van het werkelijke publiek bij elke post
- Tekst Facebook & Advertenties
- Tekst Facebook & Werknemer
    - Wat met andere institutionele partners (verzekeraar, overheid, academische onderzoeksinstelling)
    - Interessant om hier voor te waarschuwen bij/tijdens/na posts?

+ Bevragen wat hen zou tegenhouden om zulk een tool te gebruiken

5.1.12. Visualisations

Afgeprinte visualisaties, stap per stap overlopen, vragen wat duidelijker kan. Helpt dit je? Geeft dit je meer inzicht? Is dit beter dan wat al voorhanden is?

Pen en papier voor aan te duiden wat er nog mist.

6.Bibliography

Barth, Adam, Anupam Datta, John C. Mitchell, and Helen Nissenbaum
2006 Privacy and Contextual Integrity: Framework and Applications. *In* Security and Privacy, 2006 IEEE Symposium on P. 15–pp. IEEE. http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=1624011, accessed July 3, 2015.

Brunton, Finn, and Helen Nissenbaum
2011 Vernacular Resistance to Data Collection and Analysis: A Political Theory of Obfuscation. First Monday 16(5). http://firstmonday.org/ojs/index.php/fm/article/viewArticle/3493, accessed July 3, 2015.

Campani, Marco, and Ruggero Vaglio
2015 A Simple Interpretation of the Growth of Scientific/technological Research Impact Leading to Hype-Type Evolution Curves. Scientometrics 103(1): 75–83.

De Wolf, Ralf
2015 Privacy in a Networked Life. Vrije Universiteit Brussel.

Heyman, Rob, and Jo Pierson
2014 The Changing Faces of Facebook and Its Colonisation of Lifeworld. Under Review.

Hildebrandt, Mireille, Martin Meints, Denis Royer, and Claudia Diaz
2006 FiDis D7.7 - RFID, Profiling and AmI. Status: Published.

Linden, Alexander, and Jackie Fenn
2003 Understanding Gartner's Hype Cycles. Strategic Analysis Report N° R-20-1971. Gartner, Inc. http://www.ask-force.org/web/Discourse/Linden-HypeCycle-2003.pdf, accessed September 29, 2015.

Nissenbaum, Helen
2004 Privacy as Contextual Integrity. Washington Law Review 79(1). http://papers.ssrn.com/sol3/papers.cfm?abstract_id=534622, accessed July 3, 2015.

Petkos, Georgios, Symeon Papadopoulos, Thomas Theodoris, et al.
2015 D6.1: USEMP Privacy Scoring Framework - V1. Project Deliverable.

Pierson, Jo
2012 Online Privacy in Social Media: A Conceptual Exploration of Empowerment and Vulnerability. Communications & Strategies 4(88): 99–120.

Pierson, Jo, and Rob Heyman
2011 Social Media and Cookies: Challenges for Online Privacy. Leo Van Audenhove, ed. Info 13(6): 30–42.

Pötzsch, Stefanie
2009 Privacy Awareness: A Means to Solve the Privacy Paradox? *In* The Future of Identity in the Information Society Pp. 226–236. Springer. http://link.springer.com/chapter/10.1007/978-3-642-03315-5_17, accessed July 22, 2014.

Rethinking Personal Data: Strengthening Trust
2012. Switzerland: World Economic Forum.

Rizos, Georgios, Symeon Papadopoulos, and Yiannis Kompatsiaris
2015 Learning to Classify Users in Online Interaction Networks. *In* . http://www.usemp-project.eu/wp-content/uploads/2015/05/rizos_iccss2015.pdf, accessed January 29, 2016.

Turow, Joseph, Michael Hennessy, and Nora Draper
2015 The TradeOff Fallacy: How Marketers Are Misrepresenting American Consumers And Opening Them Up to Exploitation. Report from the Annenberg School for Communication - University of Pennsylvania. Pennsylvania. https://www.asc.upenn.edu/sites/default/files/TradeoffFallacy_2.pdf, accessed July 1, 2015.

Van Dijck, José
2013 The Culture of Connectivity: A Critical History of Social Media. Oxford University Press.

Zimmermann, Christian
2015 A Categorization of Transparency-Enhancing Technologies. arXiv Preprint arXiv:1507.04914. http://arxiv.org/abs/1507.04914, accessed October 6, 2015.