D4.1

Social Requirement Analysis – V1

V 1.4 / 2014-08-18

Tom Seymoens (iMinds-SMIT), Sanne Ruelens (iMinds-SMIT), Jo Pierson, (iMinds-SMIT), Laurence Claeys (iMinds-SMIT)

This document presents the methodology used and the results of the first user research. Through an analysis of the existing Privacy Enhancing Tools and the different privacy strategies employed by users it proposes some insights into the underlying mechanisms of the privacy paradox, taking into account issues of awareness and capabilities. In the final part of this deliverable a first concretization of the gathered insights into a list of social requirements for the USEMP tool will be deduced. The methodology used was desk research, a small-scale survey and focus group interviews.

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 4	TODO
Deliverable lead org.	USEMP
Deliverable type	Report
Authors	Tom Seymoens Sanne Ruelens Jo Pierson Laurence Claeys
Reviewers	Katja de Vries (ICIS) Steven Strachan (CEA) Symeon Papadopoulos (CERTH) Adrian Popescu (CEA)
Version	1.2
Status	Draft | PMB Final Draft | **Final**
Dissemination level	**PU: Public,** PP: Restricted Program; RE: Restricted Group; CO: Confidential
Due date	2017-07-31
Delivery date	2014-08-18

Version	**Changes**
1.1	Initial Release
1.2	Theoretical part Privacy Paradox + Survey
1.3	Focus group interviews + revisions
1.4	Social Requirements

Table of Contents

1.Executive Summary

The overall goal of Work Package 4 is to enhance our understanding of how users make use of Online Social Networks in their every day life, in light of the development of a Privacy Enhancing Tool: the USEMP-tool.

The main research question guiding our user research was the following: How can we **enhance user empowerment** in a rising **culture of connectivity** by identifying, understanding and strengthening the social and technological aspects of **user tactics** coevolving with platform strategies?

In the first chapter of this deliverable we pay special attention to the concepts that underlie this research question such as the culture of connectivity, user empowerment and the privacy paradox: the paradoxal phenomena that many users might be concerned about their privacy online, but do not make use of the available means to restrain the possible risks. In its core, this concept holds a division between the **attitude** of a user (his/her privacy concern) and his/her **behaviour**. From this dichotomy we deducted our four subquestions.

We continue with presenting our analysis of the existing **Privacy Enhancing Tools**, such as Privacy Feedback and Awareness Tools (PFA) and Temporary Media Tools (TMT) in the second chapter of this deliverable. We studied their affordances, practices, challenges and obstacles.

The remainder of this document reveals the first track of the user research where we explore people's **attitudes, awareness,** (declared) **behaviour and** (declared) **capabilities** regarding their online privacy. We focus on their **institutional privacy** and the strategies that they currently apply to preserve it. We also determined whether they are aware of the existence and make use of the PETs that we analysed before.

This first research track consisted of an **online questionnaire**, which was distributed in Sweden and Belgium and 4 **focus group interviews** with a total of 21 respondents. We will present the methods used and give an overview of the most important results.

The results will in turn be translated into a first version of the **social requirements**, which should function as a guideline for the technical partners and designers to further develop the USEMP-tool that addresses privacy problems by empowering users without overburdening them.

2. Design of the User Research

In this chapter, we start by briefly describing the guiding concepts: culture of connectivity, user empowerment and privacy paradox. This is necessary for fully understanding the scope of the research questions, which are listed at the end and guide the remainder of this deliverable.

2.1. Culture of Connectivity

In her book, The Culture of Connectivity: A Critical History of Social Media, José van Dijck takes a look at social media from a technical, social, economic and cultural perspective (Van Dijck, 2013). She describes how since the turn of the millennium two big transformations have taken place and how this has affected our experience of sociality.

The first transformation Van Dijck distinguishes is the one from a 'Participatory Culture' to a 'Culture of Connectivity'. The concept of 'Participatory Culture' was born in the nineties. It had to reflect the Internet's potential to nurture connections, build communities and advance democracy. It was a need for *connectedness* that drove users to the web in the first place. In the beginning of the new millennium more and more people started using websites for making and maintaining connections, by sharing creative content and enjoying their social lives online. As people's lives became more and more permeated with social media platforms, they started to move their social, cultural and professional activities to an online environment. Van Dijck notices that existing or new information companies incorporated the existing social platforms. These companies were not so much interested in the ideals of the Participatory Culture, as they were in the data that the users delivered, as a by-product of maintaining connections online. They made use of algorithms that engineer and manipulate the social connections. This is what Van Dijck calls *connectivity*: an automated process behind the real-life connections, which made it possible to recognize people's desires. As such, a profitable form of sociality has been created. This transformation goes hand in hand with the second one: from a networked communication to a platformed sociality. As the online platforms were no longer sheer carriers for communication, human sociality was being brought to these platforms and at the same time mediated by them.

The Culture of Connectivity is a culture where perspectives, expressions, experiences and productions are increasingly mediated by social media sites (Van Dijck, 2011). It's this mediation and manipulation of social relationships and the gathering of people's preferences that influenced the privacy of individuals online. Mere outings of sociality online have become structured and tracked, they are released on an electronic platform which can have far-reaching and long-lasting effects (Van Dijck, 2011, p. 7).

2.2. User Empowerment

User empowerment is a concept that is charged with meaning, described by Zimmerman and Rappaport (1988) as the process of strengthening individuals, by which they get a grip on their situation and environment, through the acquisition of more control, sharpening their critical awareness and the stimulation of participation. To provide a better understanding of how we use this expression in this deliverable we take a look at Pierson's definition when he explains user empowerment in relation to social media as the capability for interpreting and acting upon the social world that is intensively mediated by mass self-communication (Pierson, 2012, p. 103). Note the link of this definition with how José van Dijck proposed her views on the culture of connectivity.

The process of strengthening individuals, among other things, by which they get a grip on their situation and environment, through the acquisition of more control, sharpening the critical awareness and the stimulating participation.

Pierson distinguishes three main issues that need to be dealt with before one can become empowered. He starts with describing issues of inclusion. The proliferation of social media isn't necessarily equal to a growth in user empowerment, since some users are not capable, willing or permitted to get involved and participate by means of or through digital media (Pierson, 2012, p. 103). He continues by outlining issues of literacy, as not all users are capable of getting involved because they might not have the needed (digital) skills. The last types of issues one might encounter on her/his way to user empowerment are issues of privacy. This related to how aware people are towards the monitoring, processing, analysing and commodification of their digital activities by third parties (Pierson, 2012, p.104).

In the culture of connectivity where our social lives are increasingly mediated by social media, people don't always own the necessary capabilities to optimally interpret and act upon other people and institutions for acquiring an equal position in society (Pierson, 2012, p.104). In this lies a risk of disempowerment that is visible in issues of social media, privacy and surveillance.

2.3. Privacy Paradox

In a ‘Culture of Connectivity’, as explained above, there is a growing need for the protection of our privacy. Norberg, Horne & Horne (2007) mention the development of new technologies as having a great effect on this evolution. Current technology is getting more and more effective in storing and analysing vast amounts of personal data and consumer info, while the costs for doing this consistently decrease. Moreover it’s increasingly feasible to store the information for an indefinite time. Other consequences of the digitalisation of information are the ease by which it can be combined with other data and how it can reach larger and scattered audiences without much effort (Pötzsch, 2009).

These characteristics hold several potential problems. One of them being the ‘recontextualization of self-disclosure’. Taddicken describes this as follows: "When a user discloses personal information on the Internet, it is unclear to him who and how many persons are included in the audience due to temporal and spatial separation" (Taddicken, 2014, p.250). This may be the cause of **social privacy issues**, as well as **institutional privacy issues (**De Wolf et al., in press; Pierson, 2012). The first kind may happen when a user uploads certain sensitive pictures on a social network site and they become visible beyond the intended audience, while the second type may occur when those pictures get used for advertising by the social network site itself or other third parties (Taddicken, 2014). The division between social and institutional privacy was originally defined by Raynes-Goldie's. She defined institutional privacy as the concern about how third parties will use personal data.

Given such unwanted consequences, one might expect users of online social networks to be cautious when providing personal information online. Many users even state that they are concerned about privacy in general (Pötzsch, 2009). However it has been observed that people’s actual behaviour do not correspond to these claims regarding their own privacy (Deuker, 2010). These discrepancies between their claimed **attitude** towards privacy and their actual privacy **behaviour** is called the **privacy paradox** (Barnes, 2006).

Deuker (2010) proposes three reasons that might help explain this apparent paradox; he calls them the dimensions of the privacy paradox. As a first dimension, he puts forward that privacy decisions often are made on **incomplete information**. Users might for example not be fully aware which of their information is being observed, stored and processed and how this information can be linked with other sources of data to infer information that they haven’t explicitly provided. A second dimension he mentions is that most users do not have the cognitive capabilities to process all the necessary information about privacy risks to make an objective conclusion. This is called **bounded rationality** or the inability to process all the risks connected to disclosure (Acquisti & Grossklags, 2005). For the latter Deuker (2010) refers to two psychological traits. The first one is that users usually invest more time in risks for which the negative consequences become instantaneously apparent. The second one is that people often make a cost-benefit analysis before making a decision. The benefits for using for self-disclosure on the Internet are often better advertised: building and maintaining social relationships, convenience, personalised services whereas the cost (loss of privacy) might not be so clear (Pötzsch, 2009). Aiming for **immediate gratification,** it is often more tempting to give some personal information if you immediately benefit by gaining certain content or service in exchange. The perspective that users disclose information to achieve interpersonal benefits, rather than minding the harm online social network providers and other third parties might cause, is also confirmed by other scholars (De Wolf et al., in press; Young and Quan-Haase, 2013; Braendtzæg, 2010; Raynes-Goldie, 2010; Tufekci, 2008).

Taking a look at these dimensions, we can address some of these issues by raising the subject's **privacy awareness**. We follow Pötzsch (2009, p.228) definition of this concept when he describes it as the individual's attention, perception and cognition of:

- Whether others receive or have received personal information about him/her, his/her presence and activities,
- Which personal information others receive or have received in detail
- How these pieces of information are or may be processed and used, and
- What amount of information about the presence and activities of others might reach and/or interrupt the individual.

Is privacy awareness raised, the user can make decisions based on objective information and may seek the help of **privacy enhancing tools** in order to mitigate potential risks more easily. They will not do this if they are not able to identify the risk, or if they are not sure that the cost of searching, installing etc. of a PET is justified (Deuker, 2010).

Young & Quan-Haase (2013) claim that the privacy awareness for social privacy is higher than that for institutional privacy. They also see this reflected in the behaviour of users, so that the privacy paradox is more present with regard to institutional privacy issues. They found that a lot of people already apply privacy strategies, such as using private chat for sharing sensitive information or consciously not sharing information with a certain social group. This could be explained due to the fact that social privacy issues are brought quicker to their attention as they can monitor how their audience responds to their posts, while it is harder to monitor their institutional privacy. This might indicate a necessity to make the institutional and economic processes behind data sharing more transparent in order to change users' behaviour.

A last, obvious, factor for explaining the privacy paradox is that the users must possess the right skills to change their behaviour. Privacy enhancing tools might be provided, but if the users do not have the **capabilities** to employ them, their behaviour will not change, despite becoming more concerned.

2.4. Research Questions

The theoretical framework presented in sections 2.1-2.3 is represented in the research questions we tried to answer during this first user research. We aimed at getting more insights on people's **attitudes, awareness, (declared) behaviour and (declared) capabilities** regarding their online privacy with the focus on **institutional privacy**, and privacy enhancing strategies with the focus on **privacy enhancing technologies**.

This leads us to our main research question: ***How can we enhance user empowerment in a rising culture of connectivity by identifying, understanding and strengthening the social and technological aspects of user tactics coevolving with platform strategies?***

We derived following research subquestions:

1. Are people **aware** of their online institutional privacy and of possible technological ways to address this (via PET's)?
   a. Are people aware of the platforms' operational and economic logic, i.e. how and from what premise connective media (like Facebook) work?
   b. Are people aware of the existence of Privacy Enhancing Technologies (PETs) or Privacy Awareness and Feedback tools (PFAs)? Why (not)?

2. What is the **attitude** of people towards their online institutional privacy and of possible technological ways to address this (via PET's)?
   a. What is the opinion of people regarding the platforms' operational and economic logic, i.e. the premises on which the functionalities of social platforms (like Facebook) work?
   b. What do people think about current PETs/PFAs?
   c. How would the ideal PET/PFA look like from a user perspective?

3. What are the **capabilities** of people towards online institutional privacy and towards PETs?
   a. What are the skills of people to adjust or resist undesirable operational and economic strategies of connective media platforms?
   b. Are people able to efficiently and effectively use PETs?

4. How do people **behave** regarding their online institutional privacy and towards PETs?
   a. What are the user tactics we can identify in the behaviour to adjust or resist undesirable operational and economic strategies of connective media platforms?
   b. Do people currently use PETs? Why (not)?

To answer the defined research questions, we executed a mixed method research strategy. We first performed a desk research on exiting PETs. Afterwards we questioned customers in a quantitative and a qualitative way, using an online survey and focus group interviews to gather more in depth insights and explanations. All research phases were performed in collaboration between user researchers in Sweden (LTU) and Belgium (iMinds).

3. Desk Research: Privacy Enhancing Tools

There are two options for eliminating the privacy paradox, as described in the previous chapter. Either the behaviour of people changes to match their attitudes, or their attitudes need to be adapted to their actual behaviour. Pötzsch (2009) points out that only the first option can be pursued in order to enhance the subject's privacy and empower the user. Besides applying the more conventional privacy strategies, such as consciously not posting certain information or entering fake information, users can employ technological solutions like Privacy Enhancing Tools (PETs). These tools have been developed with the purpose of mitigating risks that are connected to the disclosure of personal data (Deuker, 2010). They aim to support privacy without restricting functionality of the system (Hendrik, Sunday, & Oludayo, 2013).

Since one of the primary outcomes of the USEMP project will be a tool that hands users the appropriate means to be easily informed about their (institutional) privacy status, a logical first step in our research is the analysis of existing privacy enhancing tools.

In our analysis, we differentiate between three general types of tools. The first type is called 'Privacy Feedback and Awareness tools' or PFAs. These tools make people more aware of the extent of their personal data sharing and the mechanisms behind it. They do this by providing feedback on e.g. current privacy settings, trackers that follow the users on the Internet, the business model behind online social networks etc.

Our second type of tools, we put into the common denominator of 'Temporary Media Tools' or TMTs. They are all smartphone applications that allow users to send each other text or media files that can self-destruct after a given time. Moreover these tools often also encrypt the messages or provide means for anonymous, pseudonymous, unlinkable or untraceable communication (Deuker, 2010).

The third type are end-user programming tools and human-based computation games. They will be analysed in the coming months.

The analysis of the PFAs and TMTs was performed by desk research. First of all, a non-exhaustive list of privacy enhancing tools was put on the wiki of the USEMP-project. Here, the different project partners could add tools that they thought might be relevant to investigate in light of the creation of our own architecture. After a reasonable amount of tools were gathered, a list of categories was created on which the analysis of each of the tools was done.

Subsequently, researchers from both LTU and IMINDS separately evaluated the tools in this list on 13 different parameters (see table 1). In this manner, the results could be compared to each other, in order to obtain a greater scientific reliability. The analysis was performed throughout April and May 2014.

In the next paragraphs we present our analysis of the PFA and TMT tools. A table with the complete analysis is included as an annex to this deliverable (See 8.1 and 8.2). Our analysis was updated until June 2014.

3.1. Privacy Feedback and Awareness Tools

First we discuss the PFAs. These tools have the basic functionality to inform users about the (invisible) processes underlying their personal information sharing, like identifying the companies that track their data or what do their current privacy settings entail. The hypothesis for these tools is that by making privacy issues on the Internet more manifest, the user becomes more aware of them, which may alter his behaviour or narrow the privacy paradox. We distinguish 22 different tools in this category, which were systematically analysed, based on 13 different parameters.

	Tool		Parameters
1	F-Secure Safe Profile	1	Year of Launch
2	Reclaim Privacy	2	Updated until …
3	Trend Micro Privacy Scanner	3	Type of Supplier
4	ESET Social Media Scanner	4	Tool Type
5	AVG Privacy Fix	5	Login Type
6	AVG Privacy Fix Family	6	Privacy Type
7	SimpleWash	7	Tool Action
8	Privacy Awareness App	8	Privacy as …
9	Disconnect	9	Personal Value Estimation
10	Collusion	10	Amount of Users
11	Facebook Disconnect	11	Language Availability
12	G Disconnect	12	Cost
13	Secure.me	13	Type of Use …
14	ZoneAlarm Privacy Scan		
15	Lightbeam for Firefox		
16	Privacy Check		
17	Facebook Privacy Watcher		
18	We Know What You're Doing		
19	e-Reputation		
20	Datacoup		
21	Bitdefender Safego		
22	Privacy Badger		

Table 1: Overview PFAs and Parameters

Two parameters that need clarification are 'Privacy Type' and 'Privacy as …'. In research about privacy on the Internet, often a difference is made between '**institutional privacy**' and '**social privacy**' (see above). Institutional privacy relates to users losing control and oversight of OSNs' collection and processing of their information(Seda Gürses & Diaz, 2013), whereas social privacy is meant to reflect the problems that emerge through the necessary renegotiation of boundaries as social interactions become mediated by OSN services (Seda Gürses & Diaz, 2013). The second parameter refers to the distinction between (Diaz & Gürses, 2012):

- **Privacy as control**: Technologies that provide the means to users to control the disclosure of their personal information
- **Privacy as confidentiality**: Technologies that create a new autonomous space (e.g. encryption) to prevent data disclosure
- **Privacy as practice**: Technologies that make the flow of personal information more transparent

All PFAs were developed in the current decade. The oldest one still in use (Facebook Disconnect) was made available in 2010. All these tools are regularly updated, except for two (Reclaim Privacy; Bitdefender Safego).

We could distinguish four types of **suppliers**: commercial organisations, individuals, research and government. The majority of the developers were commercial businesses (16), three of them were individuals (Privacy Check; We Know What You're Doing), three were coming from research projects or universities (Privacy Awareness App; Lightbeam for Firefox; Facebook Privacy Watcher) and one was developed on behalf of the city of Paris (e-Reputation). This distinction is interesting because this enabled us to present tools from different suppliers to our participants of the focus groups at a later stage. Using this distinction we got insights in the type of supplier they preferred and why.

We also took a closer look at the different platforms for these tools. For this we made five different groups: Android applications, iOS applications, browser plugins, computer programs and Facebook applications. It was surprising to see that only one of them was an application for an Android smartphone (Trend Micro Privacy scanner). Browser plugins and Facebook apps were the most common form for PFAs; they were both nine times present.

Type of Privacy			Privacy as …			Personal Value Estimation	
Social	Institutional	Both	Control	Confidentiality	Practice	Yes	No
11	8	3	13	0	9	2	20

Table 2 : Overview distribution PFAs over different categories

Most of the PFAs we examined were designed for coping with social privacy issues. As to the distinction between privacy as control, privacy as confidentiality and privacy as practice, we see that only three of the tools concerned with institutional privacy have privacy as control as a characteristic (AVG Privacy Fix, AVG Privacy Fix Family; Privacy Check). The tools dealing with social privacy issues all have privacy as control as a characteristic, except one who can be placed under privacy as practice (Privacy Awareness App). If we follow Young & Quan-Haase's statement that a lot of users already make use of specific privacy strategies to keep their social privacy issues within bounds, then there is still a lot of room and need for a tool that gives users a means for protecting their institutional privacy (Young & Quan-Haase, 2013). Moreover, only two of the tools give a value estimation of how much the users personal data is actually worth (AVG Privacy Fix; Datacoup). This kind of feature might help to create awareness about the economic reality behind online social networks and personal data.

Finally we observe that all of the PFA tools are free to use. We didn't analyse the existing business models behind these free tools, but it is for sure interesting to investigate if users are willing to pay for a means for protecting their privacy online.

In the table in annex 8.1 we indicate the amount of users for each PFA. This is an estimate by the providers themselves or based on how many times it has been downloaded, so it is not be advisable to make statements based on these (possibly biased) numbers.

3.2. Temporary Media Tools

Temporary Media tools or TMTs are tools that allow users to send private messages by making sure that their messages/identity are kept secure from external parties. Most of these tools have the function to self-destruct the texts or media that were send after a specific amount of time, hence the name. If we use again the distinction between privacy as control, privacy as confidentiality or privacy as practice (see above), we can categorize these tools under privacy as confidentiality: technologies that create a new autonomous space (by means of e.g. data encryption) to prevent data disclosure, such as personal identifiable information. We systematically studied 13 of these tools on 13 parameters.

	Tool		**Parameters**
1	Snapchat	1	Year of Launch
2	Confide	2	Updated until …
3	Telegram	3	Type Supplier
4	Secret	4	Tool Type
5	The Wut App	5	Login Type
6	Popcorn Messaging	6	Privacy Type
7	Privatext	7	Tool Action
8	CoverMe	8	Encryption
9	TigerText	9	Amount of Users
10	Wickr	10	Language
11	Silent Circle	11	Cost
12	Burn Note	12	Type of Use
13	ZipaClip	13	Type of Media

Table 3: Overview TMTs and Parameters

All TMT tools were developed in the current decade (just like the PFA tools). The oldest one we analysed, Snapchat, was launched in 2011. All of them are getting regular updates.

Similar to the PFAs, the majority of applications were dealing with social privacy issues. Only five of them, specifically claim to provide a strong enough form of encryption, to guarantee absolute protection from data collection (Privatext; CoverMe; TigerText; Wickr; Silent Circle).

Opposed to the PFA tools, all of the suppliers of the TMTs were commercial businesses. Also the platforms used for TMT tools are different. All of them are smartphone applications. Ten tools were available for both Android as iOS systems, three were only available for iOS (Popcorn Messaging; the Wut App; Secret) and only one tool, had a web-based equivalent (Burn Note).

All TMT tools except one had the possibility to make a service specific account. The Wut App was the only exception on this. For this application you had to login with your Facebook account, which raises questions on privacy issues. Aware of this, they market their product as semi-anonymous.

Most of the TMTs focus on the transfer of texts. Some also make it possible to send pictures (Snapchat; Telegram; Secret; Privatext), video (Snapchat; Telegram; ZipaClip) or sound (Telegram) to recipients in encrypted format. Two applications also offer the possibility to call to other users in a secure and private way (CoverMe; Silent Circle).

In the table in annex the amount of users for each TMT is included. However this is an estimate given by the providers themselves or based on how many times it has been downloaded. It is not advisable to make statements based on these numbers.

4. Survey

4.1. Methodology

Our main research questions for this first user track aim to provide insights on the **awareness** and **attitudes** toward online institutional privacy on one hand, and control-taking **capabilities** and **behaviour** on the other. The first step for acquiring these user insights was the set up and execution of a quantitative survey, in the light of gathering first descriptions of:

1. Background information (using validated scales) on and general topics of interest within the context of our research questions,
2. Information on the use of PETs by the user group.

The survey consisted of 12 mixed multiple questions and 15 matrix questions with a 7-point Likert scale, was built with the Qualtrics[1] software, and took approximately 15 minutes to complete. Between 10 June and 16 June 2014, the questionnaire was sent via e-mail to all students of the Bachelor in Communication Sciences at the VUB, grade 1 through 3, as well as students of the International Master Program, in total around 250 students should have gotten the invitation to participate. The invitation for participation to the survey was also send around via a tweet from the Twitter account of Communication Sciences Department of the VUB and the University of Ghent. The low response rate can be explained by the timing, as the invitation to participate was sent after the final exams had ended. Of the 58 respondents who participated, 93 per cent (n= 54) completed the survey.

The invitation to participate briefly explained the USEMP project and the subject matter of the questionnaire. Those who decided to take part in the survey therefore knew the topic regarding privacy risks on the Internet and PET tools. An incentive was included in the invitation, as participants had the opportunity to win a €20 voucher of a popular multimedia retailer in Belgium.

LTU in Sweden sent out a similar survey. Their questionnaire consisted of 29 mixed multiple choice and open questions. Data was gathered between 9 April and 14 April 2014. Of the 55 members who participated, 85 per cent (N = 47) completed the survey. They have reported their results in a report titled: ‘Summary of questionnaire to understand different aspects of user's online privacy and awareness of privacy enhancing tools’.

In the remainder of this chapter we will look at the results of the survey that was send out by iMinds. Where it was possible, results are compared with the LTU/Botnia-survey.

4.2. Participants

4.2.1. General demographics

As shown in Table 1, women and people in their twenties were dominant in the study, with respectively 82 and 76 percent. The mean age of participants was 26 years and ranged from 18 to 43 years old. This resulted in a vastly different group of respondents than the Swedish,

[1] http://www.qualtrics.com/

where males and those over 30 years of age (the mean age there was 36) were dominantly represented.

Demographics	**Belgium (n=54)**	**Sweden (n=47)**
Gender		
Male	10	34
Female	44	13
Age (yrs)		
<20	5	0
20-29	41	15
30-39	6	11
≥40	2	21

Table 4: Demographic Characteristics of Belgian and Swedish Respondents

4.2.2. Media Ownership and Social Media Use

Ownership of digital media was high amongst the Belgian respondents, yet smartphone use was slightly lower than the respondents of Sweden. The desktop computer and mobile phone proved to be the least popular devices to own, whereas the entire group of respondents owned a portable computer (or laptop). Table 2 represents the percentages of respondents who own digital media, as well as their use of social media.

Media Ownership & Social Media Use	**Belgium (n=54)**	**Sweden (n=47)**
Owned Medium		
Smartphone	81,5	97,87
Tablet	35,2	
Desktop	13	
Portable Computer	100	
Mobile Phone	25,9	
None of the Above	0	
Social Media Use		
Yes	100	89,36
No	0	10,64

Table 5: Digital Media Ownership and Social Media Use of Belgian and Swedish Respondents (in %)

Amongst the 54 Belgian respondents, there were no non-users of social media. When asked which social media channels they had used in the previous month, four types stood out: social networking sites, video channels, collaborative wisdom projects and conversation applications. As shown in figure 1, and parallel with results from Botnia, the least popular social media according to our results were crowdfunding, multiplayer virtual (game) worlds and crowdvoting platforms.

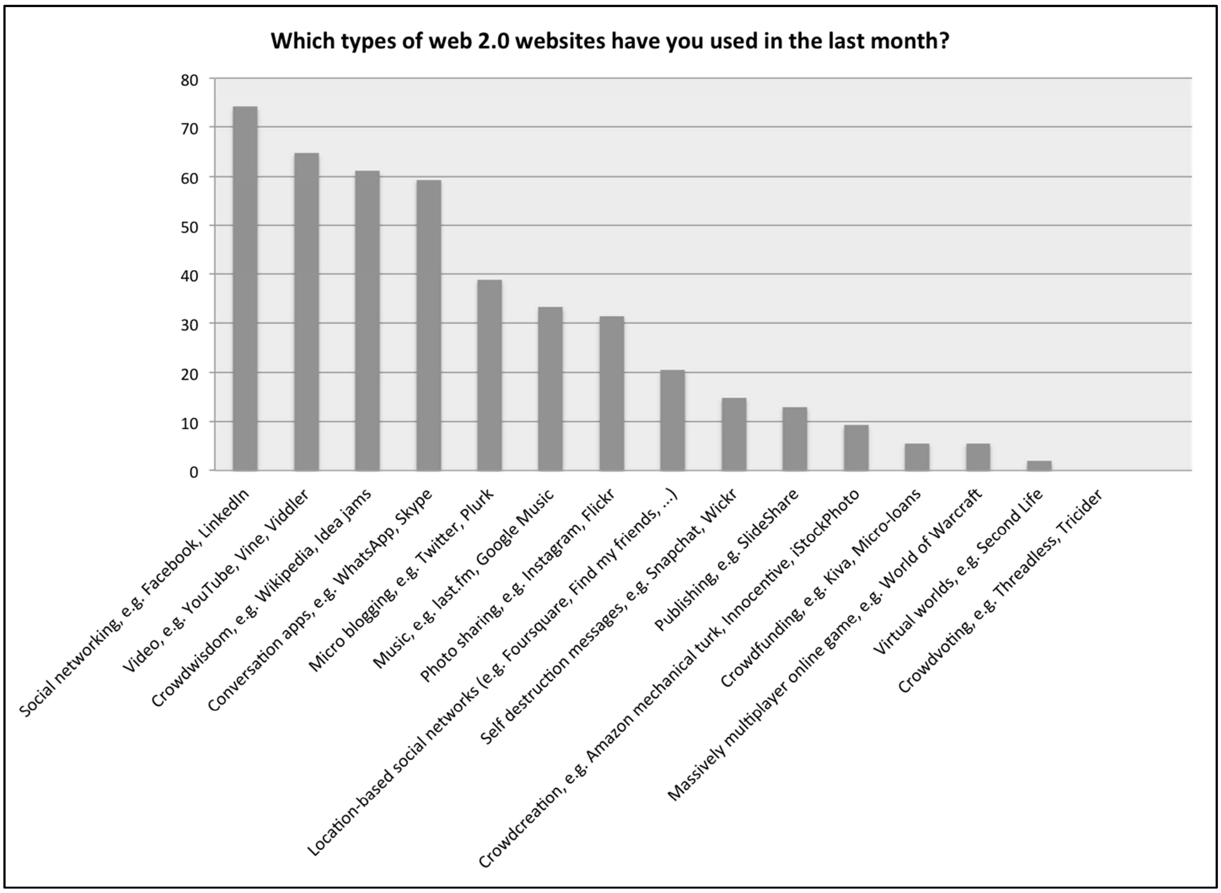


Figure 1: User Engagement per type of Social Media %

4.2.3. Trust Stance and Social Awareness

Participants were asked to indicate their level of agreement on four statements concerning (physical) trust, by arranging a slider ranging from 1 till 7 (7 being the highest level of agreement). This because former research showed that there is a correlation between the (physical) trust stance and the online trust level of people (Willaert & De Graaf, 2014). In the respondent group trust levels of participants showed no signs of outliers, with the concept of 'granting people the benefit of the doubt' being most commonly agreed on. Women were, albeit slightly, more trusting than men, especially regarding initial physical trust and the honesty of human nature (see figure 2).

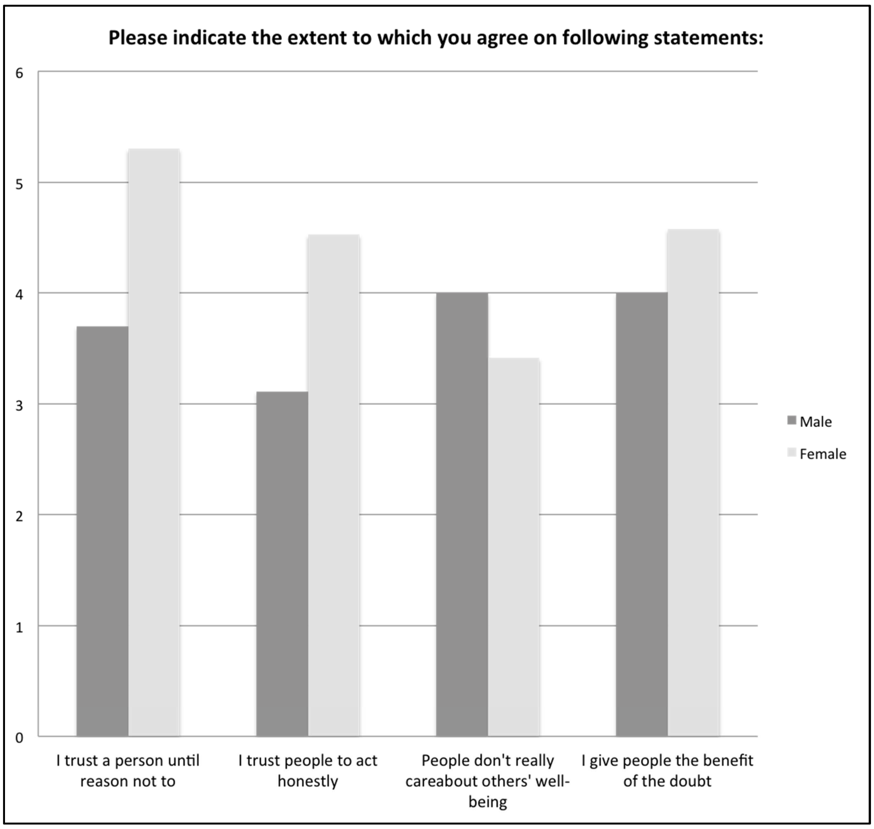


Figure 2: Level of Physical Trust: Gender Comparison (Mean results on a 7-point scale, n=46)

Dinev & Hart (2006: 11) found strong support for the hypothesis that Internet users with high social awareness will not only follow Internet privacy issues more closely, but will stress the importance of privacy as a societal value as well. They proposed 6 items concerning engagement and interest in social issues and developments in the community, which we consecutively used to measure the social awareness of our respondent group.

Participants showed high levels of agreement with the statements, especially on following developments within the community and discussing social issues with others. The only exception concerned interest in government regulation of high-tech business (see figure 3).

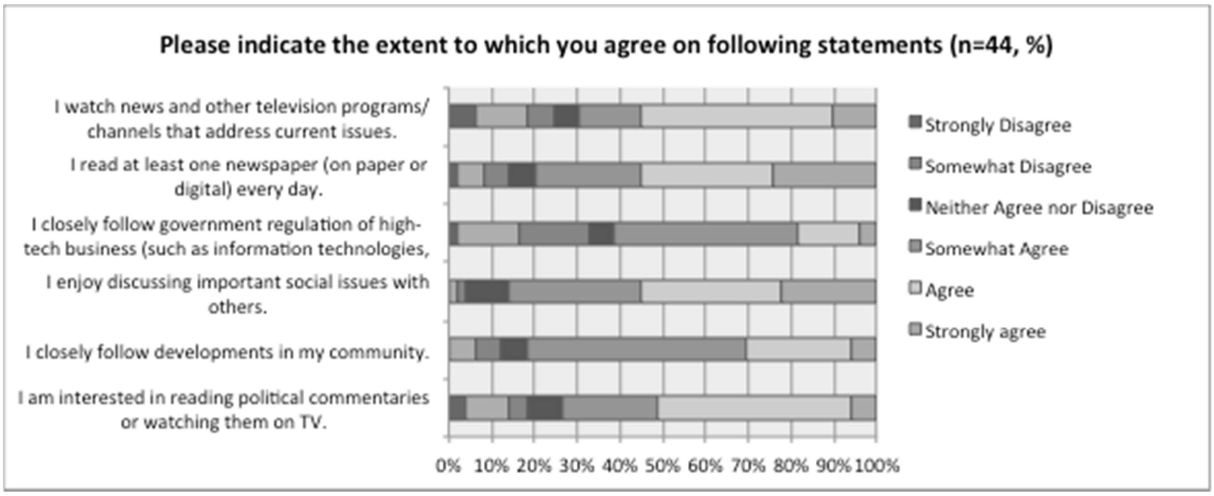


Figure 3: Level of Social Awareness (n=44, %)

4.3. Trust on the Internet

4.3.1. Internet Skills

Internet skills, as defined by van Deursen (2010), entail four skill types and range from basic product skills to understanding the characteristics of the medium and useful coping techniques. For measurement of the Internet skills of our respondents, 20 relevant items were derived from van Deursen's more elaborate scale (2010: 130). Using a frequency scale, ranging from never to daily, we aimed to measure operational, formal, information and strategic Internet skills.

Formal Internet skills were seemingly high, as feelings of disorientation and getting lost online were almost never experienced. Informational Internet skills, such as using multiple search keywords; and operational Internet skills, such as using the refresh button, were also used frequently (with the exception of downloading of programs). In general, respondents claimed to benefit from using the Internet on daily or weekly basis. However, this did not include financial benefit. In general we can state that the internet skills of our participant group was rather high.

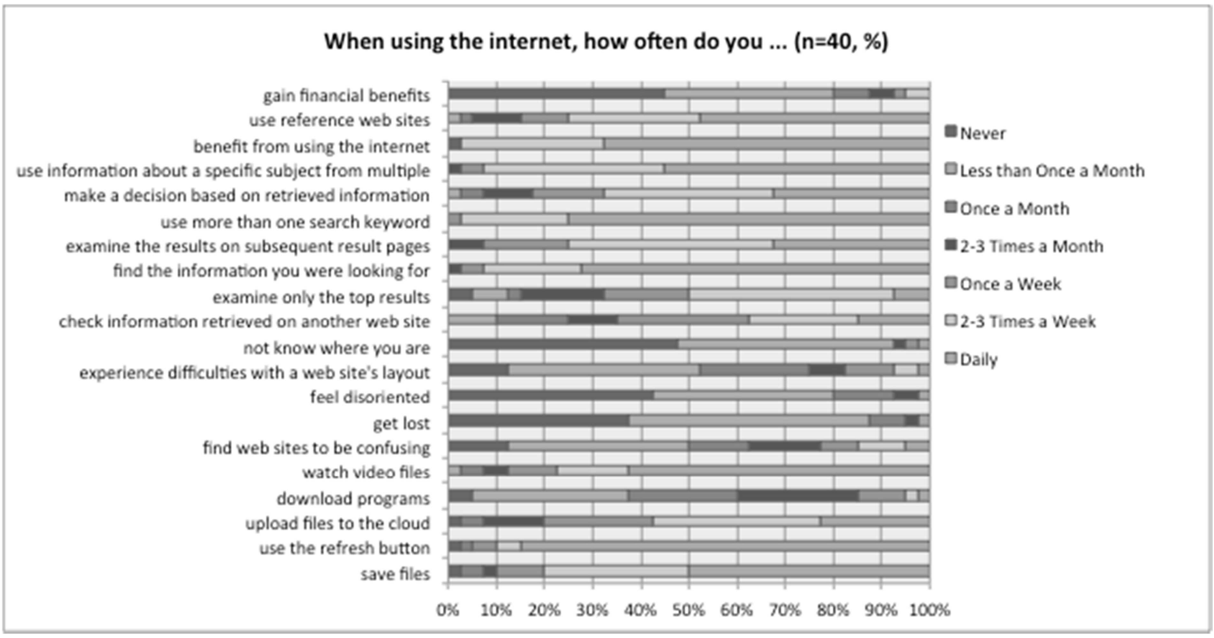


Figure 4: Internet Skills based on Frequency (n=40)

4.3.2. Trust Related Seeking Behaviour

In an online environment, people might express trust related seeking behaviour when interacting with institutions. This can go from a mere location check, to reading the fine print of a corporate website's disclaimer. Based on the framework of trust formation in organizational relationships (McKnight et al, 1998) and reworked by Willaert & van der Graaf (2014), respondents were asked to rate the occurrence of seven trust related search actions in order to assess the level of their trust related seeking behaviour.

Most prominent information seeking behaviour involved the reputation and location of an institution, as well as the confidentiality guarantee of provided data. Legislation and liability regarding online interactions were rather uncommon. Perhaps surprisingly, trust marks or seals of approval were rarely sought after (see figure 5).

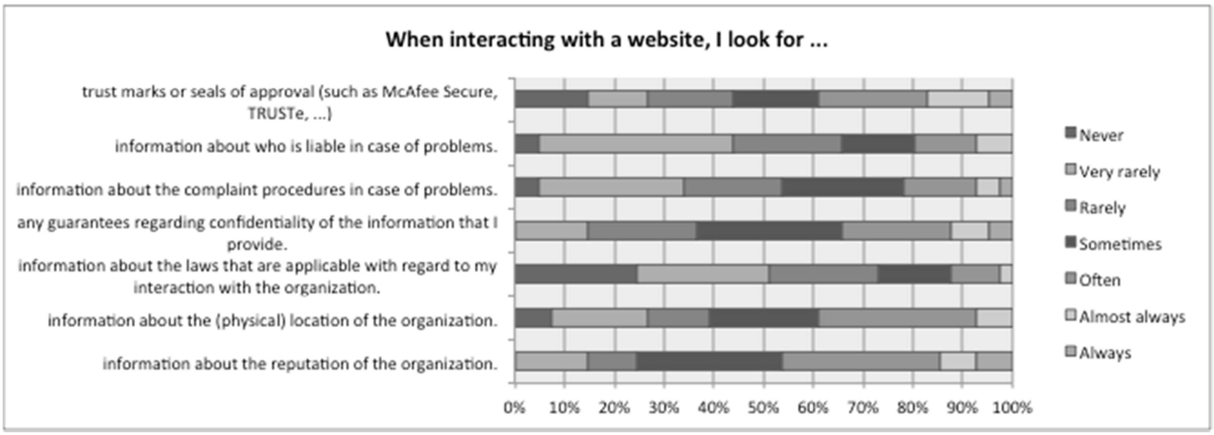


Figure 5: Level of Institutional, Trust-related Seeking Behaviour (n=41, %)

4.3.3. Trust Related Consequences

Not only trust seeking behaviour, but also trust related competences were queried in the survey. Four statements on institutional privacy capabilities were scored, ranging from strongly agree to strongly disagree. Results showed that our respondents did not seem to feel confident about their online competences when it comes to privacy. Even though most of them claimed to understand their rights and duties when using an online application, the three remaining statements were met with more insecurity. Agreement with the ability to detect when personal information has been misused or when a third party has gained access to the app, appeared to be largely absent (see figure 6).

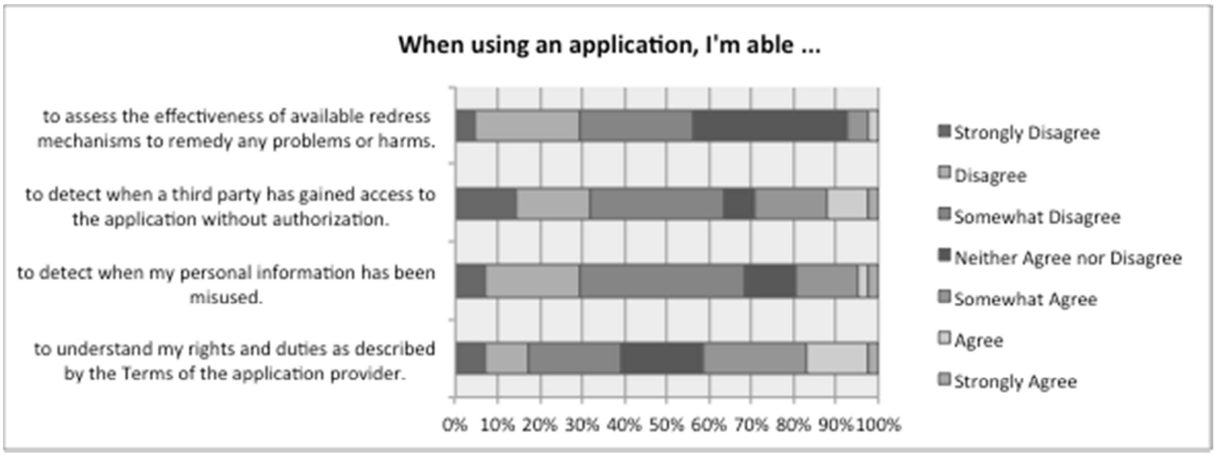


Figure 6: Trust Related Competences (n=41, %)

4.4. Opinions on Online Privacy

4.4.1. Privacy Concern

Making use of a validated scale from previous work (Krasnova et al, 2009), attitudes towards online privacy, privacy concern and use of personal data by companies were measured. Similar to the results in Botnia, the majority of the users acknowledge the existence of overall threats to their online privacy.

As depicted by figure 6, only a minority of respondents (13%) is not concerned about threats to their personal privacy. Others feel it is an important force to reckon with and are sensitive to the way their personal information is dealt with by third parties.

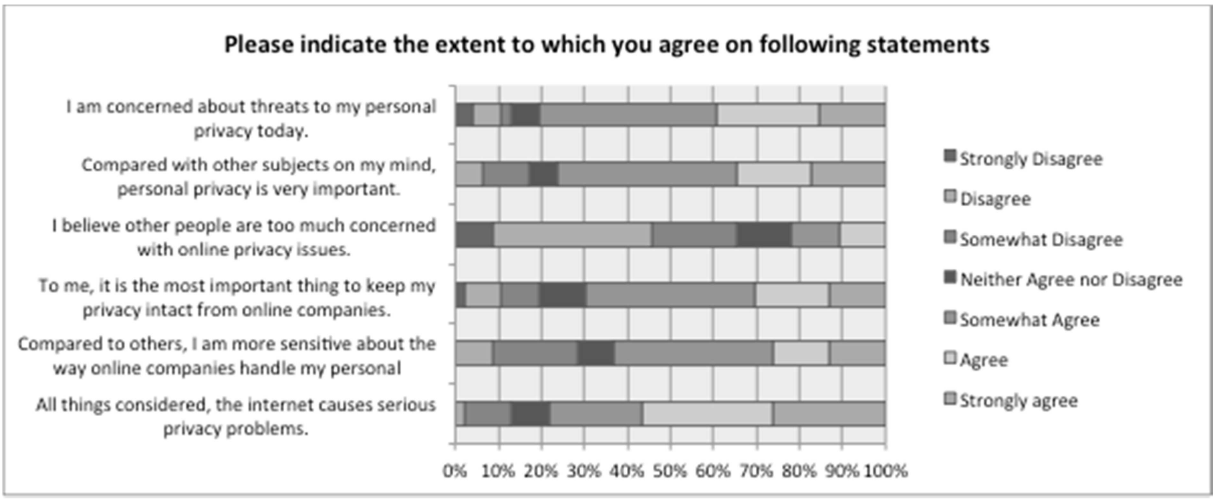


Figure 7: Attitudes on Online Privacy (n=46, %)

4.4.2. Online Institutional Trust

When asked about their opinion on the trustworthiness of certain types of online institutions (on a 7-point scale), it seems that online banking and governemental services were trusted most. Social networks on the other hand, even though they were used by all participants, were trusted the least (see figure 8).

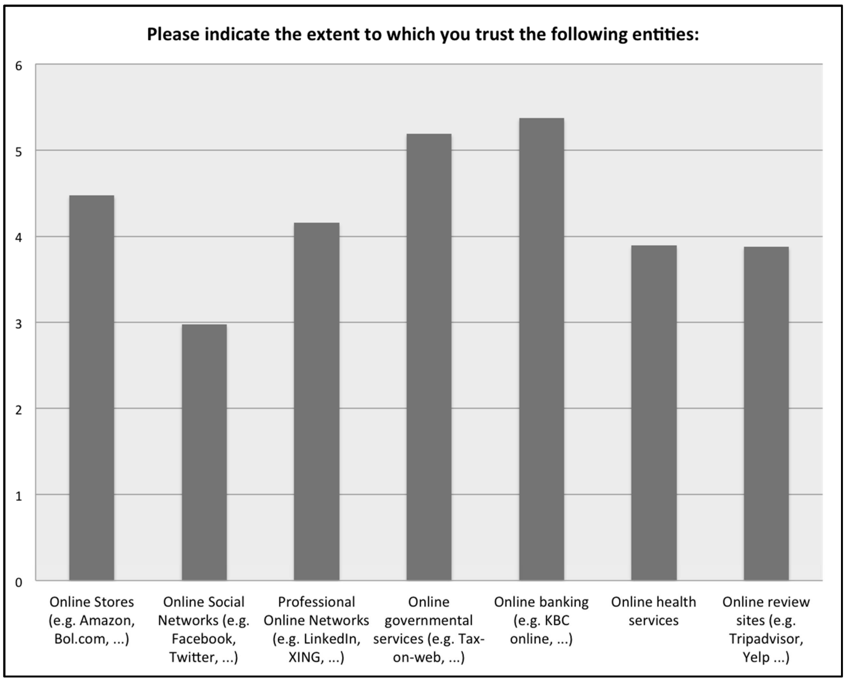


Figure 8: Online Institutional trust (Mean Results)

When breaking down these scores per age category, it is noteworthy that people under the age of 20 are inclined to find nearly all institutions more trustworthy than older generations.

This is especially true for social networks. Respondents in their twenties and thirties seem more critical when judging organizations (see figure 9).

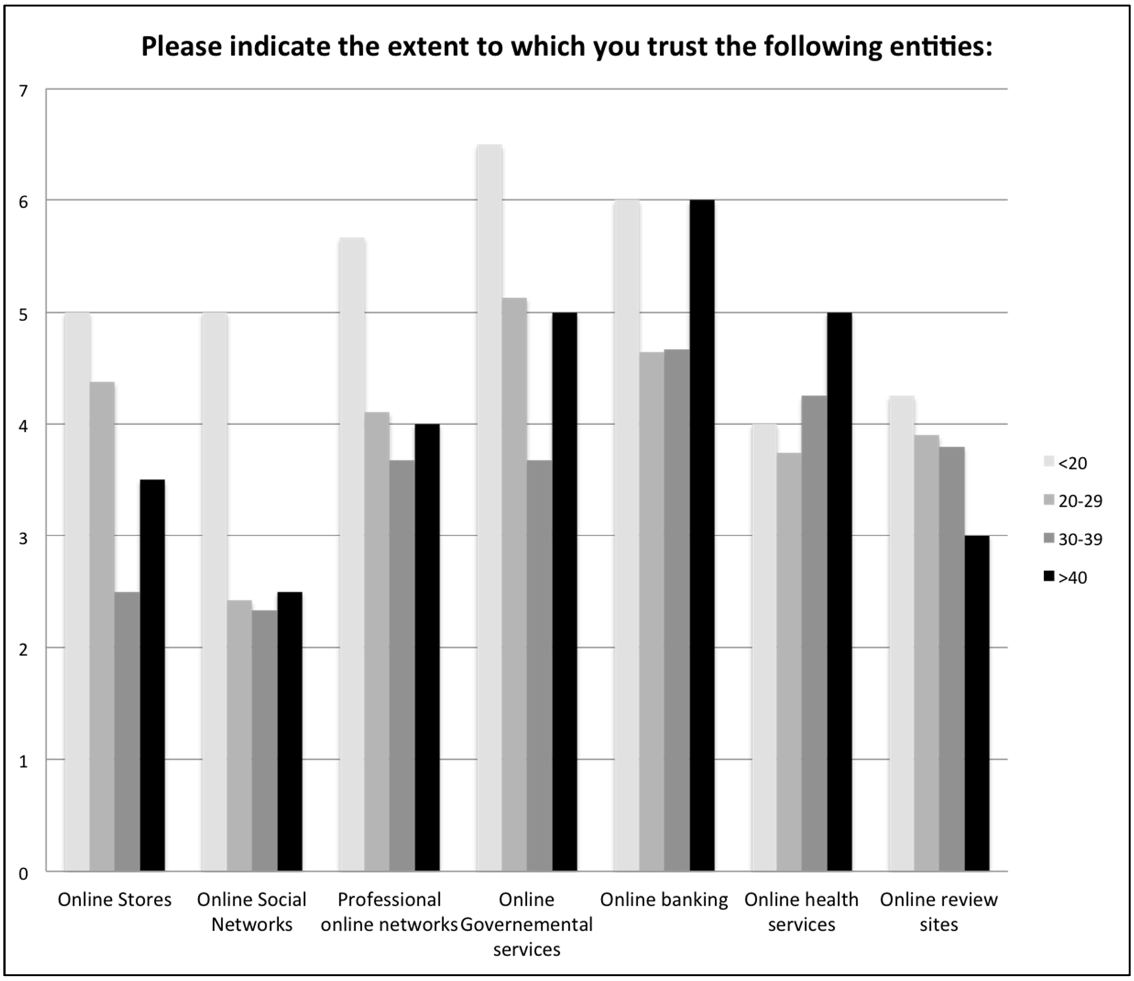


Figure 9: Online Institutional trust per Age Category (Mean Results)

4.5. Online Social Networks

Facebook Use (n=40, %)	
Yes	97,5
No	2,5

Table 6: Facebook Use (n=40, %)

With 100% of our respondents using social networks, and 98% using Facebook, the following two questions regarded individual privacy management. To probe respondents about privacy management actions, for social media in general as well as specifically for Facebook, we introduced two scales as developed by De Wolf et al (2014). Proposed actions were to be scored on a 7-point frequency scale and included actions that represented basic, advanced and appearance privacy management.

The results of social media privacy management in general showed that privacy settings and providing incomplete information were most commonly used. On the other end of the spectrum, using fake personal information and asking others what to do regarding data protection were used rarely, if ever (see figure 10).

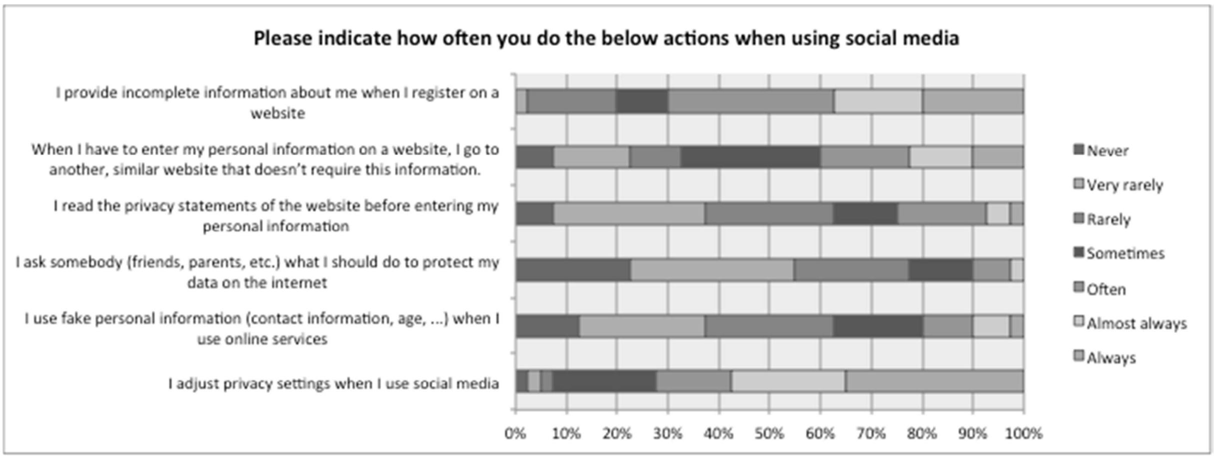


Figure 10: Individual Privacy Management Online (n=40, %)

Privacy management actions for Facebook resulted in, maybe surprisingly, quite a high level of agreement on statements regarding appearance management (De Wolf et al, 2014). This could however be attributed to the high number of 20- to 29-year olds in the respondent group. Basic management actions such as allowing only friends to view personal profiles, not filling in all information inquired by Facebook and being careful who to accept as friend are most agreed upon. Reviewing and untagging photos also rank high in the results. Making use of Facebook lists when posting and defriending people are actions that are disagreed with the most (see figure 11).

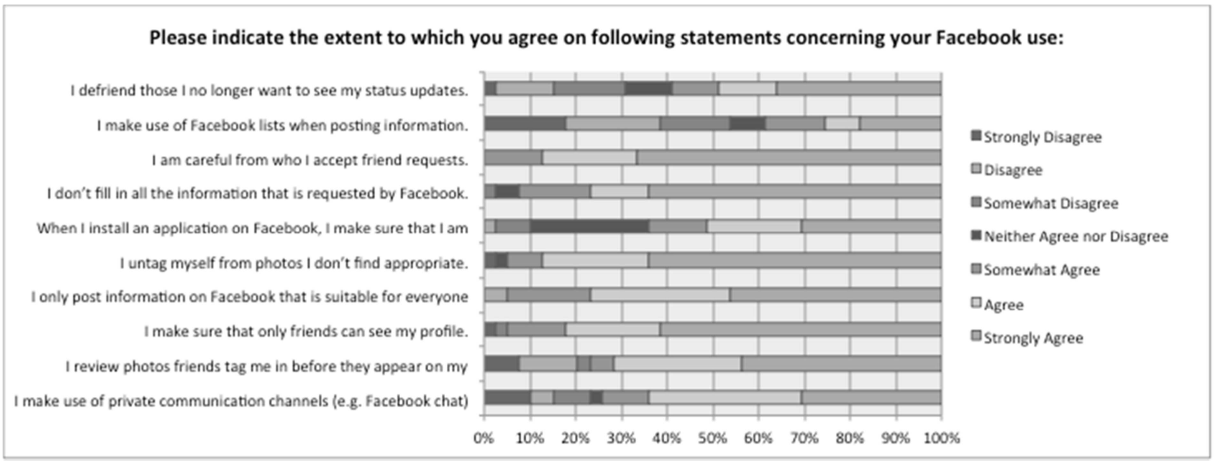


Figure 11: Individual Privacy Management on Facebook (n=39, %)

When considering online privacy on Facebook, it is not always a matter of individual control as others are inherently part of the equation. Respondents were asked to score to what extent they consider the behaviour of others as an uncontrollable social risk to their own privacy management on social networks. As shown in figure 11, there is indeed a noticeable concern about the lack of control on behaviour of others. In some cases, respondents were slightly less bothered by others posting photos or content about them online, however this seemed to be influenced by age. Older age categories (those over thirty) agreed it bothered them, whereas the younger categories tended to disagree with these statements (especially those under 20 years of age).

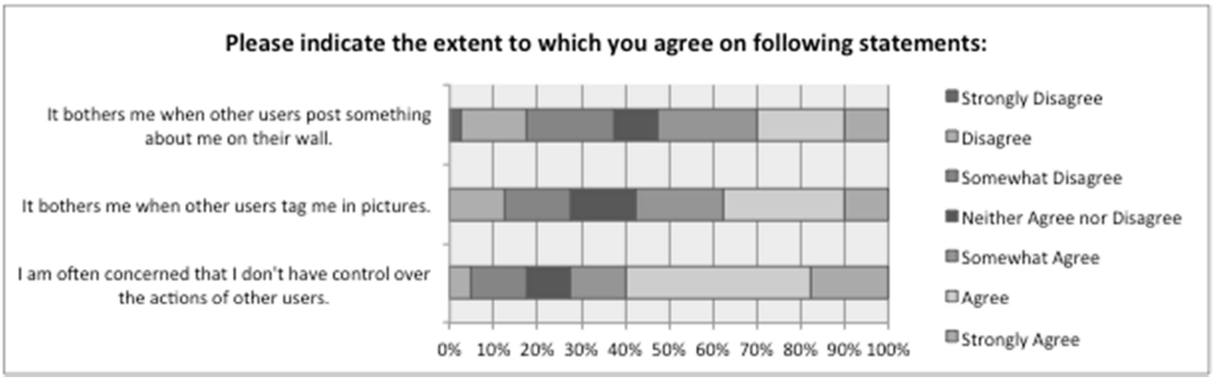


Figure 12: Uncontrollable Social Risks (n=40, %)

4.6. Privacy Enhancing Tools

4.6.1. PETs

PET Awareness	
Yes, and I have used them before	40
Yes, but I have not used them before	27,5
No	32,5

Table 7: PET Awareness

Many, yet not the majority of respondents were unfamiliar with privacy enhancing tools (32,5% in Belgium, as opposed to 48,9% in Sweden). However, an even larger percentage of the Belgian respondents have used them before (40%). Awareness of PETs was higher amongst men (only 11% of men was not aware of PETs opposed to 39% of women) and heightened with age (see figure 13). Reasons respondents indicated for not having used a privacy enhancing tool were: not being fully aware of them, not being sure they needed one, presuming they are too complex and finally, laziness.

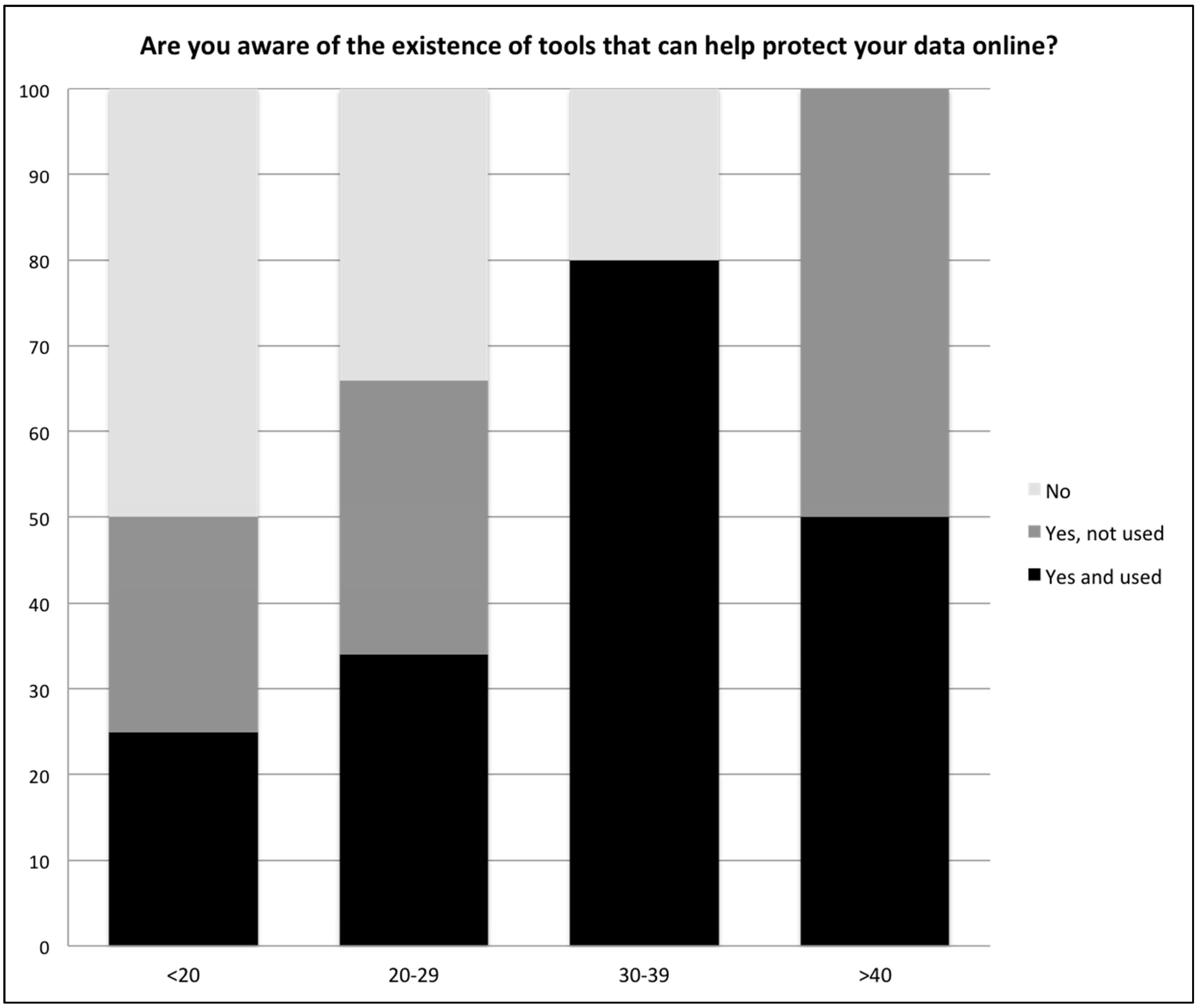


Figure 13: PET Awareness and Usage per Age Category (n=40, %)

Similar to the results from Sweden, many PET tools were unknown to our respondents; with encrypted voice/video, anonymous remailers and publishing tools as the top three PETs our respondents had never heard of. PETs that seemed slightly more popular, both in awareness and usage were cookie/cache/Internet history cleaners, VPN accounts, anonymous search engines and anonymous browsers.

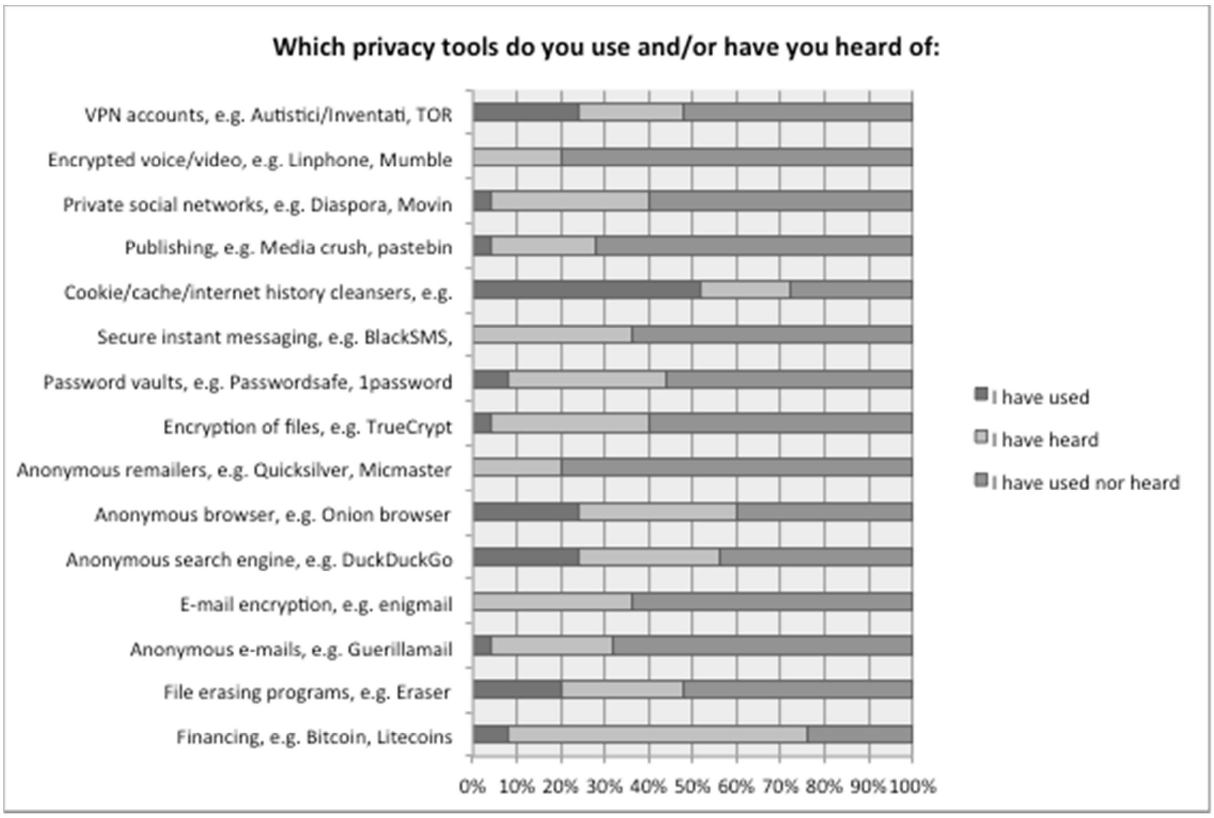


Figure 14: Awareness of Different Types of PET (n=25, %)

PET Satisfaction (n=17)	
Level of Satisfaction	
Very Dissatisfied	5,9
Dissatisfied	23,5
Neutral	52,9
Satisfied	11,8
Very Satisfied	5,9
PET sufficient to protect privacy?	
Yes	0
No	64,7
I don’t know	35,3

Table 8: PET Satisfaction (n=17)

When PET users were asked to score their satisfaction of the tools, only 17,7% stated to be either satisfied or very satisfied with the product. The majority of users were either neutral or dissatisfied. Moreover, nobody felt that using a PET was sufficient to protect his or her privacy.

4.6.2. Privacy Feedback and Awareness Tools`

PFA Awareness	
Yes, and I have used them before	10,5
Yes, but I have not used them before	13,2

No	76,3

Table 9: PFA Awareness (n=38)

With 76% (and 59% in Sweden), the majority of respondents have never heard of PFA tools. Only 10% of respondents had ever used a PFA tool. The most well known tools were AVG Privacy fix and Disconnect. The only tools that had been used by our respondents are FB Sale Profile, Disconnect, ZoneAlarm, Lightbeam and Privacy check (see figure 15). With 75%, dissatisfaction of PFAs was very high. Main reasons attributed to non-use were: not being aware of PFA existence, uncertainty as to needing one, and once again, being too lazy to use one.

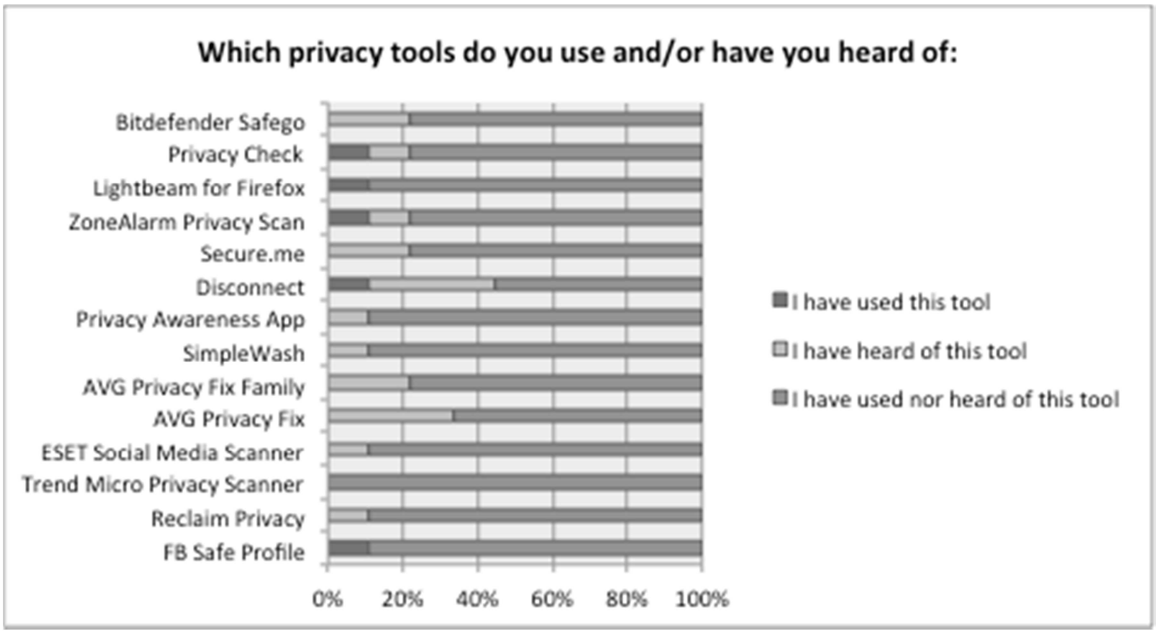


Figure 15: Awareness of Different PFA Tools (n=9)

4.7. Conclusion

As required for the T4.1 deliverable of USEMP project, a survey was conducted to explore current usage of Privacy Enhancing Tools (PETs). To broaden the scope of the survey results, questions were added which could form primary insights on our research questions and will eventually lead to reporting on the social requirements of the USEMP tool.

The survey was divided into four main sections including background information, opinions on privacy on the Internet, Internet and social media use and privacy tool use. Even though the results of the survey are not generalizable to the population, below we list our main findings, keeping our research questions in mind:

Awareness and attitude: Given our group of socially aware and trusting respondents, results indicated corresponding awareness of Internet privacy threats. However, this did not translate to lowered trust levels of most online entities, with the important exception of online social networks. The existence of PETs and PFAs, as well as the different types of tools were known only vaguely and were mostly considered insufficient by the data subjects. The survey indicated that women and people under 30 years of age were more likely not to be aware of PET and PFA existence.

Capabilities and behaviour: Despite elevated privacy concern, trust related seeking behaviour and competences were not exceptionally high. Even though many personal privacy management actions seemed well established on social media networks, actual usage of PETs was not.

5.Focus group Interviews

Alongside the previously discussed quantitative survey, which provided descriptive information on e.g. user knowledge and use of PETs, we applied a qualitative research strategy to gather more in depth information. Four focus group interviews were conducted to receive a deeper understanding of users' privacy awareness, attitudes, behaviour and capabilities. As this is our first qualitative exploration of users within the project, we preferred the use of focus groups over interviews. Our main motivations for this method were to be able to explore one specific theme, in this case privacy, in-depth with a variety of people. In a setting that stimulated participants to respond to and act on each other's views, new insights and perspectives were expected to emerge more easily than in an individual interview setting. Also, a discussion in a group would challenge the participants to explain and verbalize their views very accurately (Bryman, 2012) in order to get their point across, allowing us to capture the sensitivities and nuances of what they really meant.

5.1. Focus group design

Four focus group interviews were conducted in Dutch throughout the first two weeks of July 2014. We made a distinction based on age: two focus groups were with young participants (from 18 to 25 years), and two other focus groups consisted of participants between 35 and 45. In total 21 people participated to the focus groups.

Pseudonym Respondent	Age	Work Situation
Anne	25	Looking for employment
Elliott	24	Student Political Sciences
Sarah	22	Student Teacher
Josephine	22	Student Teacher
Eva	22	Student Office-Management
Jack	24	Software Developer
Catherine	22	Student, Bio-Sciences
Joni	24	Living Lab Researcher
Willy	28	Engineer Bio-Chemics
Bob	23	New Media Researcher
Timothy	24	Student Industrial Engineer: ICT
Philippe	22	Student Computer Sciences
Chris	43	Embedded Developer
Jean	44	Policy Officer Education Innovation
Jessica	43	Communication officer
Arthur	41	Security Manager
Stephanie	43	Housewife
Paul	34	ICT coordinator
George	37	Principal of a School
John	40	Software Developer
Keith	35	IT Consultant

Table 10: Overview Participants (Pseudonimised)

To recruit respondents, we relied on the expertise of iMinds' living lab organization iLab.o. Our aim was to have a panel of six respondents per group, so taking into account the probability of unexpected (and unannounced) cancellations, we over-recruited. As an extra incentive, we provided the user with a voucher of €30 for a Belgian retail chain for books and multimedia. Our approach resulted in an attendance that was only slightly lower than our initial target, with between four and seven people present for all focus groups. All respondents signed an informed consent. In this document we situated the USEMP-project and we stipulated that all information would be pseudonimised and handled with great care, this document can be found in the annex of this deliverable (See Annex 8.5).

The focus group sessions took place at the offices of iMinds in Ghent (Belgium). We preferred to hold the sessions in a research environment to install trust amongst the participants. The duration of a session was on average 2 hours and took place after 18h30 in order to optimize attendance for respondents who came straight from work.

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

1. Short introduction, explaining the voice recording of the session and the general outline of the focus groups (20")
2. Gathering insights on the respondents' general thoughts on privacy (10").
    a. By asking open questions about privacy in general and the perceived difference between offline and online privacy.
3. Gathering insights on the respondents' awareness and attitude towards privacy online (20").
    a. First, we showed the participants a short video for raising awareness about personal data sharing, made by the European commission.[2]
    b. We then explained the concept of 'Personal data'
    c. We asked open questions about the sharing of information online and how they tried to protect it.
    d. The respondents were asked to write down their current privacy strategies and discuss them afterwards.
4. Exploring the respondents' awareness and attitude towards the economic and operational logic behind online platforms (30")
    a. We first showed the participants by showing part of a documentary about tracking on the Internet by the Flemish public service broadcaster VRT (Eén, Koppen, 3 September 2013)[3]
    b. We asked open questions about the participants' attitudes towards data brokers, tailored advertising and protection measures.
5. Exploring the respondents' awareness, attitudes, behaviour and capabilities towards Privacy Enhancing Technologies (20")

[2] https://www.youtube.com/watch?v=BgE4JpeDGR8
[3] http://www.een.be/programmas/koppen/digitaal-goud

   a. We presented the participants with two PETs:
      i. Ghostery[4]: We chose this tool as it has a nice visualization of who is tracking you across the web.
      ii. AVG Privacy Fix[5]: We chose this tool as it has a visualization of your personal value estimation and it's made by a commercial organization.
   b. Afterwards we collected their thoughts and comments on these tools and how they would improve them.

6. Asking for possible additions and comments (10")

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

Focus Group	Date	Age Range	Participants	Location
1	01/07/2014	18-25	7	iMinds, Ghent (B)
2	03/07/2014	35-45	4	iMinds, Ghent (B)
3	08/07/2014	35-45	5	iMinds, Ghent (B)
4	10/07/2014	18-25	5	iMinds, Ghent (B)

[4] https://www.ghostery.com/

[5] https://www.privacyfix.com/

5.2. Report

In this chapter, we will report the first results of the focus group interviews. The focus groups were transcribed ad verbatim from the audio recordings. For the analysis of the transcriptions we used Dedoose[6], a web-based platform for the analysis of qualitative data. Using this tool, we added codes to different extracts of the transcribed focus group sessions. In a first step we scanned the transcripts for topics or issues that were articulated, the so-called codes. After careful consideration, different codes were linked according to recurrent themes. In an end phase, we brought codes and subcodes back to the theoretical and overarching concepts that structure this report.

This report holds the result of the primary descriptive analysis, a second - deeper - analysis will be included in deliverable 4.4: Social Requirements-v2. This chapter is structured in correspondence with our earlier formulated research questions (see 2.4). Our findings are supported with quotes, which were literally translated from Dutch.

[6] http://www.dedoose.com/

5.2.1. Privacy Awareness

In this part the privacy awareness of our participants is explored. During the sessions we wanted to see if they are aware of the tracking and commodification of personal data. Our second step was to find out if they knew about the existence of tools that can help them protect it.

A. Towards the platforms' operational and economic logic

When looking at the respondents' awareness concerning the operational and economic logic behind online platforms, we could identify two recurring themes that our data brought to the surface: **awareness towards data gathering online** and **awareness towards profiling**. Profiling is defined here as the process by which user profiles are created based on their personal data, which can in turn be offered to organisations to personalize their service (e.g. tailored advertising).

Most people expressed that they were aware that their steps on the Internet were recorded. They often first mentioned awareness towards the collecting of their volunteered data, the information they posted on the Internet.

When asked directly which types of information they thought they released on an average day, most respondents mentioned basic personal information, such as their name, age, phone number, email accounts and location.

> *Chris (fg2, m, 43)[7]: "I think this is mostly limited to your address, phone number, your date of birth, … It's impossible not to set this free."*

As the discussion continued, most respondents demonstrated awareness that their observed data was being tracked as well. This awareness was often the result **of an experience** they had in the past, which made them realise that something or someone was following their steps on the Internet:

> *Joni (fg4, v, 24): "Today I wanted to buy a new smartphone, so I quickly took a look at several websites. Facebook and Google immediately started giving me advertising for smartphones."*

Often, the experiences that made our respondents more aware were **negative ones** that resulted in disadvantages. The next excerpt demonstrates a conversation between two respondents about price setting:

> *Willy (fg4, m, 28): "At the Ryanair-website you can see the price rising when you often search for a specific flight. When your friend takes a look at the flights from a different computer, the price could be lower."*
>
> *Bob (fg4, m, 23): "How much is the difference in price then?"*
>
> *Willy (fg4, m, 28): "That depends, when I was looking for tickets to Thailand, it suddenly was* ***€****900 euro, while on my tablet the price was only* ***€****800. And they threatened me by saying that there were only two seats left, while on my tablet five were still available."*

One of our respondents carefully criticized feelings of disadvantage:

[7] (focus group session, gender, age)

> *Bob (fg4, m, 23): "I think we are mainly confronted with our privacy when we experience its downsides. When you get the search results that you are looking for quicker on Google, it's positive. But when you get spammed with advertising about glasses that you don't really want to buy, that's negative. That's when you get confronted with it."*

When looking at the different companies our participants mentioned while talking about collecting personal data, Google and Facebook were the clear frontrunners. Besides the two companies, registration forms were recognized as a primary way for getting your info. Most people were **not aware of the existence of data brokers**, -businesses that collect our personal information, which can be used for creating tailored services. After we showed our participants, using Ghostery, who was collecting information on different types of news sites, they were surprised. Only people that were engaged in defending their privacy or had an ICT background were aware of the existence of these data brokers. They were also the only ones that expressed **a deeper understanding of how they were profiled,** based on their volunteered, observed and inferred data.

> *Elliott (fg1, m, 24): "I find it very weird that someone would be able to figure out my political views, also because I'm really careful about that."*

> *Elliott (fg1, m, 24): "It can be something very little, when you take a look at the election results and you click first on the results of the socialist party, then it could be inferred that you are interested in that."*

B. Towards the existence of Privacy Enhancing Technologies

Besides AdBlock, most people were **not aware of the existence of Privacy Enhancing Tools (PETs)**. When discussing possible explanations, some people attributed their lack of knowledge to being careful with browser-plugins.

> *Jean (fg2, m, 44): "I never heard of this. I try to avoid plugins as much as possible; in this way I can't install something harmful."*

Others feel that privacy enhancing tools should be promoted more.

> *Anne (fg1, v, 25): "I would be happy when someone would install this on my computer; it's so easy to install something wrong."*
>
> *Eva (fg1, v, 22): "Yes, it's not like they are really promoted."*
>
> *Elliott (fg1, m, 24): "That's true; things like this are often spread through word of mouth."*
>
> *Anne (fg1, v, 25): "In some social circles maybe, but that's not the case for everybody. I think I should use it if someone would explain to me how."*

This could indicate that people would use PETs more easily if someone they **trust** would recommend them. Especially for people who are not very ICT-savvy. This insight was recurring throughout other sessions:

> *Joni (fg4, v, 24): "They should be recommended by people you trust, because I don't know so much about it. For example, AdBlock was recommended by someone at work, I installed it without giving it any thought."*

5.2.2. Privacy Attitudes

As the previous section shows that most people had a certain understanding that the information they provide on the Internet could be collected, inferred and used for commercial purposes. In this part, we examine their attitudes towards this process.

In the second part we explore their attitudes towards PETs.

A. Towards the platforms operational and economic logic

In our sessions, the discussions about data collection and tailored services, often made the respondents articulate their opinions about profiling.

Generally, attitudes towards **profiling and data gathering** by corporations seemed rather neutral.

> *Jean (fg2, m, 44): "Yes, but for example, all my information is at Google and they will use it. But they don't know me personally, they only know profiles."*

Or in another focus group session:

> *Bob (fg4, m, 23): "Don't some people make too much of a scandal about it? It's not like there are people sitting at their desks at Google who are checking which mails I'm sending. I think the media kind of created the wrong image there."*

A part of our respondents also understand that for certain websites allowing their visitors to be tracked was their way of getting revenue.

> *Bob (fg4, m, 23): "What if we started to completely shield ourselves from the web, surfing without being tracked. I think that at a certain time a lot of services would disappear, because they wouldn't generate revenue anymore."*

However, when the discussion was led to **future consequences of profiling** other opinions surfaced. After showing a fragment of a documentary, where was stated that in the US some citizens had missed out on a job opportunity or a loan because of how they were categorized, participants called out for more **transparency and control**. Our participants wanted more transparency from companies towards what information placed them in which category. They also want more control over this process, as they felt wrong conclusions might be made.

> *Timothy (fg4, m, 24): "At a lot of these companies, it's not about identifying you, but about doing statistical statements. But in this way they will also categorize you, what can be harmful to you, because you are put in a box where you don't necessarily want to be."*

> *Arthur (fg2, m, 41): "If they make conclusions based on data that I can look at and correct or adjust, than that would be fine by me! Then I could say this and that is not correct because of this reason, you have to get that data out of the equation. Then I would say, ok, you can use all the data you have. But they have to show me on what information they base their decisions."*

In light of these **future consequences**, all respondents were also very aware that when they post something online, it might be there forever and could be taken out of context.

As stated in the previous paragraph, experiencing **tailored services** made our respondents more aware that their data was somehow being tracked. In their attitude towards these services, we could distinct three types of attitudes: negative, rather positive and uncertain. The first group found it **alarming** that apparently these organisations have so much information about their preferences.

> *Anne (fg1, v, 25): "No but if I (…) see advertising for job sites or universities at the side of my Facebook account, they know: 'aha, she's graduating know, she will study something else or she will look for a job' I ask myself how much do they know?"*
>
> *Jack (fg1, m, 21): "But you can use it to your advantage (…)"*
>
> *Anne (fg1, v, 25): "I don't think that weighs up (…) if I want to know something, I will look it up myself"*

A second group also found it **scary** to find out how specific some advertising was, but at the same time if the information or service was **functional,** these people perceived them as a useful advantage.

> *John (fg3, m, 40): "I receive less junk mail than in the past, because the advertising is more specific, I find them more interesting. (…) Is that a violation of my privacy? No, I think it's a positive thing."*

Finally, a third group was unsure about how to handle the topic. The following quote expresses the **duality in opinion** that these respondents held towards tailored services:

> *Willy (fg4, m, 28): "Google for example that tells me you have to take this road because there is a traffic jam. It's a little bit creepy of course that they know all this information: it's 8h30, he will get in his car or it's Friday evening he will want to watch a movie. But it's so easy as well."*

B. Towards Privacy Enhancing Tools

After we presented two Privacy Enhancing tools, Ghostery and AVG Privacy Fix, we examined our participants' attitude towards these kinds of tools. There were noticeable different attitudes across all participants.

Some of the participants favoured the tools. Stating they would like to try it, given they were user-friendly, easy to install and did not slow down their browsing experience. They also wondered why the tools did not get promoted more.

Other people received the tools with a bit more scepticism. Five categories could be deduced why some people were sceptical towards them:

1. Doubt that these tools could really stop the tracking;
2. Understanding that some platforms and services depend on tracking for creating revenue;
3. Indifference towards tracking, as long as the information only gets used to create statistical profiles and there is no 'one on one' relation, where another person knows your preferences and desires;

4. Distrust towards the business model behind these tools, especially when they were free.
5. Distrust of extra plugins in their browser that might slow down their browsing experience.

5.2.3. Privacy Behaviour and Capabilities

In this part, we will take a closer look at what our respondents declared about their privacy practices on the Internet. First we will take a look at which strategies they already apply to preserve their privacy online. After this, we will explore which types of data they are most careful with in an online environment.

A. *Privacy Protection Strategies*

Over the course of our focus group sessions, many different privacy strategies were mentioned. We will list them below with an explanation what our participants meant by them and a corresponding quote:

1) **Social Steganography**: This is the act of posting messages (e.g. on Facebook) that can only be understood by people that have the right capabilities and information to really understand it (Boyd & Marwick, 2011).

   George (fg3, m, 37): "I usually post very cryptic. (…) and only the people that have to know what I mean, can understand it (…) there's only very little amount of people that know exactly what I'm talking about. For me that's also a strategy."

2) **Audience Management**: This is the act of posting messages so they only become available to certain people. Some of our participants have divided their connections in groups; others use different OSNs for different connections (De Wolf & Pierson, 2014).

   Stephanie (fg3, v, 43): "On Facebook, for example, I divided my friends in different groups. And when I post stuff, then I decide which group can see it. I have for example, ex-colleagues, very good friends, and groups from my hobbies. I decide depending on what I post, who's allowed to see it and who's not."

3) **Using different search engines:** Some of our participants mentioned they sometimes consciously don't use Google when they want to search for a specific topic.

   Paul (fg3, m, 34): "I use different search engines, depending on what I'm looking for. So I don't put all my eggs in one basket"

4) **Private messaging:** On most OSNs it's possible to send private messages to your friends or stranger so they aren't visible for anyone who's not part of the conversation.

   Arthur (fg2, m, 41): "When I have a problem with someone, I will always say this in a private message, never in public."

5) **Withholding**: Our respondents sometimes consciously decided to not post certain information.

Joni (fg4, v, 24): "Some information I consciously decide not to share, for example I never let Facebook share my location"

6) **PET-tools:** Tools that have been developed with the purpose of mitigating risks that are connected to the disclosure of personal data.

   Arthur (fg2, m, 41): "I use AdBlock for blocking advertising, also Ghostery and Lightbeam... If I help someone for configuring his browser, I also install all those plugins."

7) **Delete cookies**: Cookies are pieces of data that are saved in your browser when you visit a website and collect information about the user that can be send back to the developer of the websites. Most browsers offer the possibility to delete them.

   Eva (fg1, v, 22): "You always have to delete your cookies when you want to buy an airline ticket (…) It seems that the more you go look, the more expensive the tickets become."

8) **Changing Privacy Settings:** Some respondents change their privacy settings on Facebook to have more control about who can see certain information.

   Eva (fg1, v, 22): "I try to adjust my privacy settings on time, for example on Facebook"

9) **Use fake/incomplete information:** An often-used tactic under our respondents was faking mandatory information in webforms.

   Catherine (fg1, v, 22): "I had to download something for school and I had to make an account and give my telephone number. I thought why do they need this? So we tried putting in only zeros."

10) **Private browsing/Incognito Mode:** Mode of browsing so the pages you view won't be in your search history or cookie store.

    Stephanie (fg3, v, 43): "I use private browsing or how do they call it? That I turn off cookies and search history so I can look up information without being followed by it afterwards"

11) **Multiple OSN accounts:** Some users have multiple OSN accounts so they can use dummy-ones when they have to login on sites they don't trust.

    Jack (fg1, m, 21): "I have an account that's completely empty and that I only use to log in to services that I don't completely trust"

12) **Multiple email accounts:** The advantage to having multiple email accounts is that you can have a formal one that you try not to spread to everyone. A such you won't feel intruded by unwanted information e.g. SPAM.

    George (fg3, m, 37): "I have three different email accounts, one I use for games, one I use for fora and the other one is my official one. In this way I try to keep all information separated."

13) **Keeping accounts separated:** When the possibility is given to create a separate account to enjoy a service, some users prefer to do this, instead of linking their social media account too much with other websites.

    Philippe (fg4, m, 22): "On every site I make a different account and I won't make use of the oh so famous Facebook or Google+ - login option. I make a separate account so these websites stay separated, for as far as this is possible."

14) **Don't use social networks:** Some users don't prefer not using OSNs as they don't want their personal data collected.

    Eva (fg1, v, 22): "For example, I know Twitter, but I also know that I won't use it actively. That's why I prefer to not have an account on this platform."

15) **Encryption of data:** This is like putting a 'lock' on your data. Only people who have the right key to unlock the data can read the information.

    Jack (fg1, m, 21): "I try to make everything as safe as possible, so no one can reach the info. That is also a requirement for my job. The applications need to be safe and when information is send over the Internet, it has to be encrypted."

Although many privacy strategies were mentioned, in reality most people only actively applied audience management, withholding, using fake information, private browsing and multiple email accounts. Whereas audience management and withholding were primarily used for social privacy issues, using fake / incomplete information, incognito mode and multiple email accounts were used for protection against institutional privacy intrusions. In the table on the next page, all strategies are listed. They are arranged according to how many times they were mentioned over all focus groups. Please note, that this is merely an indication to which privacy strategies come first to mind, it could be that some strategies that were mentioned less are being used more in everyday life. This is represented in the table as private messaging closes the list.

Amount of Mentions	Privacy Strategy	Social/Institutional Privacy
11	Using Fake/Incomplete Information	Institutional Privacy
9	Audience Management	Social Privacy
9	Withholding	Social/Institutional Privacy
7	Private Browsing/Incognito Mode	Institutional Privacy
6	Multiple email accounts	Institutional Privacy
4	Multiple OSN accounts	Social/Institutional Privacy
4	Keeping accounts separate	Institutional Privacy
4	Delete Cookies	Institutional Privacy
3	Social Steganography	Social Privacy
3	Don't Use Social Media	Social/Institutional Privacy
3	PET-tools	Social/Institutional Privacy
3	Changing Privacy Settings	Social/Institutional Privacy
2	Using Different Search Engines	Institutional Privacy
2	Encryption	Institutional Privacy
2	Private Messaging	Social Privacy

Table 11: Overview Privacy Strategies

> *Willy (fg4, m, 28): "For getting unbiased search results, I make use of private browsing. Otherwise when I need to search constantly on a specific subject, the order of search results gets changed and I get some weird advertising.*

Some respondents also gave several reasons why they were not **capable** of always consciously protecting their privacy behaviour. Some people expressed that they find this too **difficult**, or **time-consuming**:

> *Eva (fg1, v, 22): "My whole Facebook-profile is a privacy fail. I had the plan to take a look at it after my exams, but I found this to be very difficult: it takes such a long time before you can get the things off that you don't like."*

Others admit that they are so used to working with the Internet in a certain way that it's **hard to change their habits**:

> *Timothy (fg4, m, 24): "So, we have to use DuckDuckGo, they don't keep track of anything, it is the only search engine that doesn't collect your info. But I'm so accustomed to the search results that Google offers me, so I don't even use it."*

Other people just feel **powerless** towards maintaining their privacy:

> *Joni (fg4, v, 24): "There is so much that is being tracked. Even if we do little things: the amount of clicks, the amount of time we spend on a time, … that's also privacy. I don't think there's much we can do to protect us."*

B. Current use of PETs

In our small sample of respondents not much people made use of PET-tools. The reason for this is that most people were **not aware** of their existence; some are also worried they install the wrong tools and are not **skilled** enough to adequately employ them.

The PET that most commonly used was AdBlock. But some doubt was present if this was really privacy enhancing. This is nicely illustrated by the following discussion:

> *Bob (fg4, m, 23): "I use AdBlock, but is this tool privacy enhancing?"*
>
> *Timothy (fg4, m, 24): "mm, it does make you less sensitive towards intrusive advertising"*
>
> *Willy (fg4, m, 28): "But it makes you less aware after a while, you might be giving a lot of information to Zalando but you are less aware that you share so much with them because you don't receive their advertising."*

Other PETs that were used were a Heartbleed detector[8] and Firefox Lightbeam[9].

> *Chris (fg2, m, 43): "I use a Heartbleed detector. In this way I'm notified when a site has a security breach. So I know that some data I input there might get hacked."*
>
> *Arthur (fg2, m, 41): "You have to install Lightbeam and then go to some websites, you will immediately know where all your data is going and who is tracking you. It's a real eye-opener."*

[8] https://play.google.com/store/apps/details?id=com.lookout.heartbleeddetector&hl=nl

[9] https://addons.mozilla.org/nl/firefox/addon/lightbeam/

5.2.4. The Ideal Privacy Enhancing Tool: Necessities

At the final part of each focus group session we tried to get some feedback on what an ideal privacy enhancing tool would look like for the respondents. We wanted to gather input on which functionalities are necessary to include and would make them apply PETs. Furthermore, we aimed to figure out which features would discourage users.

A. Privacy Rating System

One of the features that our respondents proposed was a **privacy rating system**, a system where users could easily see how high a website/company valued privacy. A short overview of the privacy statement with bullet points and a rating system could be used here.

> *Eva (fg1, v, 22): "It's probably impossible to do this, but I was thinking about something like this: When I for example want to buy something on the internet (…) I sometimes wind up on smaller websites where I'm not sure if I can trust them. Maybe there should be stars: for example, eBay is 5 stars because they apply to certain conditions. People who use the website immediately see this rating. So it's easier to see whom to trust."*

Another user knew how Ghostery provided the option to get more information about the data brokers that are following you, like a link to their privacy statement and applauded this idea.

> *Arthur (fg2, m, 41): "That's the fun part about Ghostery: if you want more information, you can find it there."*

Most people of our focus group sessions do not read the privacy statements because of its difficult language and lengthy references to legislation. That is why they proposed that this should be available in short, clear bullet points.

> *Sarah (fg1, v, 22): "This need to be basic, just the bullet points (…) so the guy working in a Coca-Cola factory can also grasp the meaning."*

B. Estimation Value of Personal Data

One of the tools (AVG Privacy Fix), shows an estimation of how much your personal data was worth on a yearly basis for Facebook and Google. Some respondents acknowledged that this was only an estimation, but that this was a nice visualization nonetheless.

> *Joni (fg4, v, 24): "I think this can be more confronting towards the general audience, so they know what the impact is. For example, [the value of your personal data] at Facebook is for some people quite a lot. In this way you can get people to think about it."*

C. More Control: Practical Privacy Tips

In general most of our respondents indicated a need for **more control** over their data and who receives it.

One respondent mentioned that, for her, it would be useful if the tool suggested what she could do to enhance her privacy. She wanted more **practical privacy tips**.

> *Anne (fg1, v, 25): "If it would say: try to adjust this and this, change those settings, for example on Facebook. I would find it useful to receive some specific tips. In this way you can really change something."*

Another respondent wanted to be able to have control over whom he granted access to his data.

> *Willy (fg4, m, 28): "That's something that I would find interesting, if I could say, they can't have access, but they can because they give part of their profit to Amnesty or something."*

More Transparency: Real-Time Privacy Warnings

In general there was also an outcry towards more transparency on the Internet. So we could see which companies own what data and how this influences certain decisions.

> *Timothy (fg4, m, 24): "For me the big problem is that you don't know which statistics lead to which conclusions. If you would know that if you like the TV-show '24' on Facebook that you probably are always late with your payments, than you would probably not like this show. That's one of the reasons that I never like anything, I don't want to be put in such a box."*

In light of the creation of an ideal PET the following statement was made:

> *Josephine (fg1, v, 22): "Maybe something should be provided that while your busy using your computer, it gives you warnings. (…) An app that would say 'don't click on this because …'"*

Other Features

Some other necessities that were articulated were the need for user-friendliness and corresponding with this that it should not slow down your browsing experience. One user also wanted complete freedom in handling the tool, adjusting the settings to his preferences.

Most respondents also mentioned that if the tool would become too expensive, they would probably not buy it.

In light of trust towards the developer, one person would prefer if there were full disclosure of the mechanisms behind the tool. He therefore proposed to make the tool open-source.

5.2.5. The Ideal Privacy Enhancing Tool: Deal breakers

A. No real control, plain information

A concern that returned in our discussion about the ideal PET was that in the end the user would not get handed the right mechanisms for taking control over their personal data.

> *Jessica (fg2, v, 43): "It's important that you can really do something with this tool, not just show what's happening. But that you can also decide: I'm okay with this following me and receiving this data, but not with this and that (…) because what can I do when it just shows me what's happening?"*

B. Developer of the tool

One of our tools we used for probing our respondents was made by a commercial organisation (AVG Technologies). This brought on some reason for concern from some of our participants:

> *Willy (fg4, m, 28): "Actually for me AVG is a fishy company. They sometimes just give you a toolbar without asking for it."*
>
> *Elliott (fg1, m, 24): "I actually have a question: what is the business model of this tool? Because AVG sometimes bothers me a lot with all the pop ups they give: 'be careful, you are in danger of …' "*

When the participants were asked whom they would trust for making a tool or application for protecting their privacy, most respondents agreed that it should come from an independent organisation or independent programmers.

> *Arthur (fg2, m, 41): "I prefer to give my data to a group of ICT-savvy enthusiasts that develop the tool in open source without any fishy backgrounds. It would be weird to put my privacy in the hands of commercial organisation who then can track me themselves."*

In one focus group some doubt was ventilated whether or not they would trust the tool if it was officially supported by the Flemish government or European Union.

> *Bob (fg4, m, 23): "What if in the tool it would say: supported by the Flemish government or European Union?"*
>
> *Willy (fg4, m, 28): "Who says that the European Union is less fishy than the US government? They are probably full of lobbyists."*

> *Philippe (fg4, m, 22): "I recently saw a documentary about the new privacy regulation in Europe. There was a Belgian politician who asked for more than 200 extensions towards and he didn't even know it himself! Eventually Europe is just as corrupt, maybe a little less, but if there's money, there's corruption."*

C. Other deal breakers

Other deal breakers that were mentioned were a lack of user-friendliness, too difficult to use, too expensive, and when it would slow down the browsing experience.

Some respondents were also concerned that when everyone would start using this sort of technologies some services would not survive, due to lack of revenues from data brokers.

6.Social Requirements

We end this deliverable with a list of social requirements. This list is the result of the different tracks of the first user research of the USEMP project. Before presenting the results, we will shortly explain what the concept of social requirements encompasses.

Technologies don't exist in a vacuum, but they are embedded in the everyday life of their users. By applying the technologies and sharing their experiences, the users attach meaning to them. In this way both the technologies and their practices get socially constructed. In order to truly understand what drives users to certain technologies, designers have to take a look at how they are used and what this implies in terms of requirements (Gürses, 2011).

Duysburgh & Jacobs (2010) define social requirements as the users' needs related to the use of an application in interaction with others. This could mean interaction with other users as well as 3rd parties. In this case the users are regarded as a group of people that pursue a common goal, here: the protection of their personal data. The designers need to consider ways to educate users to protect themselves, while still allowing them to socially interact (S. Gürses, 2011).

6.1. Social requirements for the USEMP tools

6.1.1. Dealing with the Problem of Awareness

This section makes some suggestions towards how the USEMP tool might be able to create more awareness towards the economic processes underlying online platforms.

Although most respondents in our focus group sessions noted that they were aware that the information they provided on the Internet was collected, they initially talked merely about their **volunteered data.** There was much less outspoken awareness about the tracking of their **observed data**, let alone **inferred data**.

However, when they stopped to reflect about the **tailored services** they received (e.g. advertising), it dawned on them that obviously more information must be gathered and linked.

1. The USEMP tools should make institutional privacy problems more tangible and understandable. Right now it is 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**.

In general, the participants had a neutral attitude towards the **plain collection of their data**. Our respondents explained this by stating that the data feed statistical profiles and do not attribute values to the data subject.

By confronting them with potential **future consequences** on an **institutional level**, they became more aware that data are in fact objective, but they can get a subjective quality when decisions are based on them that influence their everyday lives.

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

Most participants could not exactly pinpoint who was tracking their data. When asked they often named Facebook and Google. Adding online shops such as Zalando that keep track of your behaviour on their sites. The majority was not aware of the existence of or the operational logic behind **data brokers**.

3. 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.**

6.1.2. Learning from current privacy behaviour

This section makes some suggestions toward how the USEMP tools might help users in maintaining or take up known privacy strategies.

Our focus group sessions revealed 15 different privacy strategies our participants used. Although in total this seems like a lot, in reality most people only actively use audience management, withholding and private browsing.

The results of our survey support that users already have some privacy strategies. They for example alter their privacy settings and review pictures on Facebook.

Three reasons that were given to not make use of the available strategies was that they seemed too time-consuming, too difficult and that it was hard consciously changing their browsing habits on the Internet.

4. 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 different search engines, have a button for deleting cookies, switching to private browsing, reviewing pictures on Facebook …

6.1.3. Dealing with the problems of transparency

This section makes some suggestions toward how the USEMP tools might give some transparency to users.

Some participants would like more transparency towards the economic processes behind their data. When showing an estimation of the value of personal data for Google and Facebook, most of them were interested but also recognized the gadget-value of such a visualization.

5. 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. This might be not feasible to realise within the scope of USEMP. Alternative solutions can be explored.

Most participants also recognized that they were not aware of the privacy statements of the different websites they used daily. Reasons given were that they were too time-consuming and formulated too difficult. Following the three dimensions of the privacy paradox (Deuker, 2010) - see part 2.3 -, one can claim that it is not possible to make conscious decisions based on incomplete information.

6. 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.

7. The USEMP tools should take into account the **different type of users related to trust-seeking behaviour**. One solution doesn't fit for all

8. 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.

6.1.4. Countering the obstacles for using PETs

This section mentions the different barriers that the project needs to tackle to promote the use of the USEMP tools.

As our survey made clear, not many people use or are aware of the existence of Privacy Feedback and Awareness tools. 76% never heard of such tools (59% in Sweden) and only 10% of the respondents had ever used one.

To get the USEMP tool adopted, the awareness of the existence and the willingness to use a PET should increase to a large extend. The analysis done on the PET tools (paragraph 3) and the outcomes of both user research tracks show this clearly. The much higher adoption of TMTs in relation to PFAs show that a clear value for the user must be embedded in the app for the user, and maybe privacy enhancement doesn't have to be the central feature of the application.

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

Our focus group sessions had the same conclusion. It became clear that only a small minority actually used them, a major reason for this non-use is that not many users were actually aware of their existence. Our participants mentioned that they are not really promoted at the moment. Other reasons were the fear off downloading the wrong plugins that could harm their computers.

10. 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.

Also some scepticism existed towards PETs. Some doubted that they could actually have an impact. This goes together with the expressed need for more control and not just information. In our survey it became also clear that of the users that actually tried a PET the grade of dissatisfaction was very high (75%).

This need for more control, besides the giving the necessary information, also implies that the users should be handed the necessary features by which she/he can effectively exert his control.

11. 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 PET-tool can become more positive**.

List of social requirements for the USEMP tools
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.
4. Supporting existing privacy strategies by taking away barriers that inhibit a widespread use.
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.
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 PET-tool can become more positive.

Table 12: Initial list of Social Requirements for the USEMP tools

7.Conclusion and next steps

In a “Culture of Connectivity” perspectives, expressions, experiences and productions are increasingly mediated by social media sites and their automated processes underlying their sociality. As a result it becomes more and more challenging for users to empower themselves in relation to their personal data. In this deliverable we explored people’s **attitudes, awareness, (declared) behaviour and (declared) capabilities** regarding their online privacy to understand how we can help users in their struggle for empowerment.

With regard to people’s **awareness,** we conclude that although they have a general sense of the economic and operational logic behind connective media, there is room for improvement. They do not seem to be fully aware of the processes behind the gathering of volunteered, observed and inferred data and how they are profiled based on this information.

Most people are not aware of the existence of Privacy Enhancing Tools.

The opinion of the respondents about the economic reality varied. Towards the gathering of information our respondents articulated an impartial standpoint, as they see this as a neutral process that doesn’t affect their everyday lives. The institutional consequences are not clear.

The majority of people that already have used PET-tools were not satisfied. The results of our survey showed us that no one felt that they were sufficient in protecting their privacy. People that were not aware of them found that they are interesting, but at the same time they were met with some scepticism. This seems to have something to do with the reputation of plugins.

In our focus group sessions we could distinguish 15 different privacy strategies that were currently used by our participants. However it has to be noted that they weren’t all used very frequently. According to the results of our survey altering privacy settings and providing incomplete information were the most commonly used user tactics.

Privacy Enhancing Tools have a low degree of usage. With only 10% of our respondents having ever applied one of them. Our focus group interviews also showed they weren’t a well-established method of enhancing privacy online. Since it was only a minority of people that have used a privacy enhancing tool, it’s difficult to say something about their capability to do so. We can mention here that some people didn’t embrace the idea of using PETs because they thought it would be too complex too handle.

For dealing with this issues we ended this deliverable by listing 11 social requirements for USEMP tools that could hold the potential of empowering the users in a culture of connectivity:

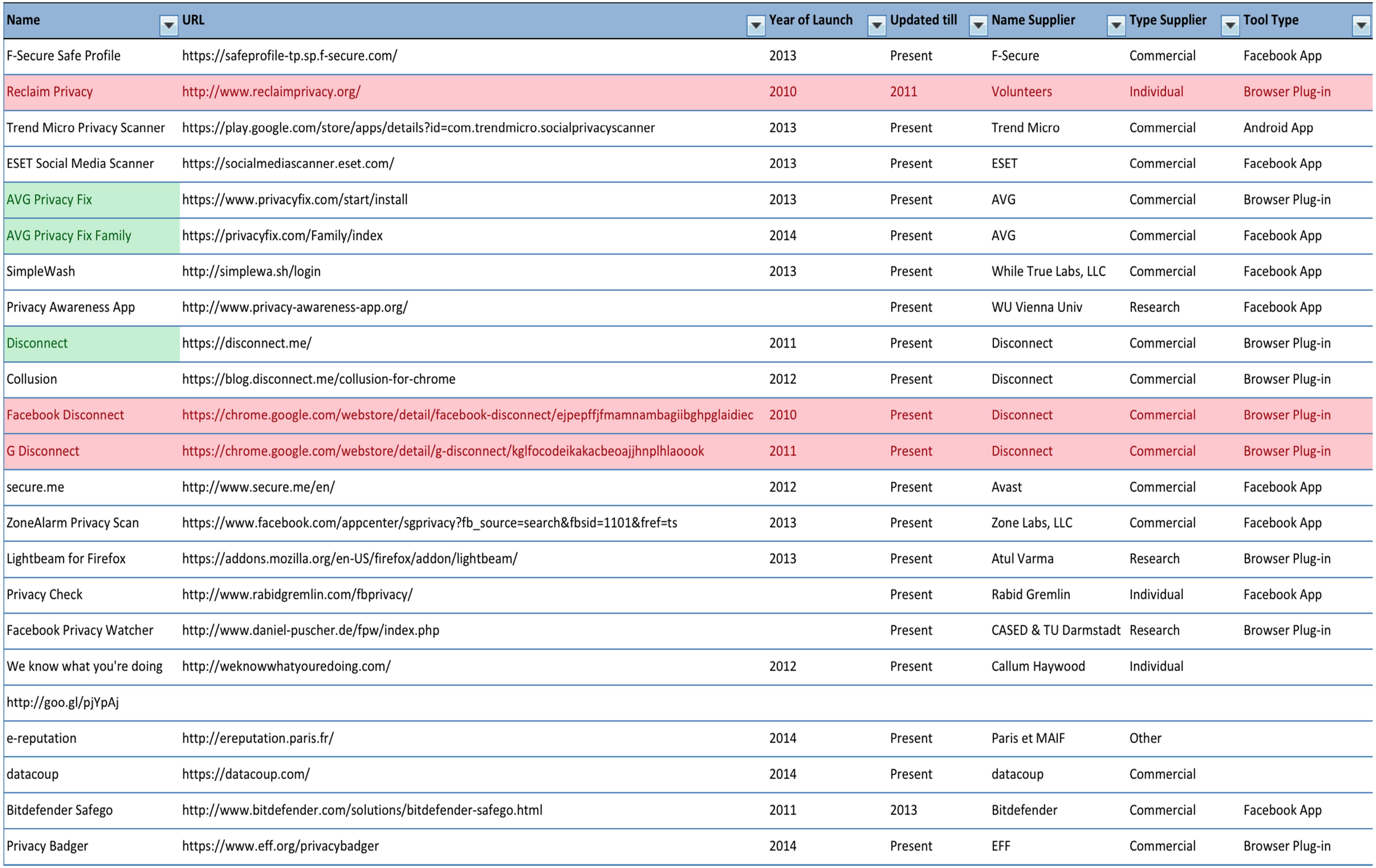
1. Linking online behaviour to known examples from the past of institutional privacy issues for raising awareness towards potential future institutional consequences
2. Presenting the user with tangible situations where user data was used for explicitly customizing a service (e.g. tailored advertising).
3. Visualizing the several data brokers and partners to which they send their data.
4. Supporting existing privacy strategies by taking away barriers that inhibit a widespread use.
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. Taking into account the diversity under the users related to trust-seeking behaviour
8. Proving the trustworthiness of the organization behind the USEMP tools to augment the adoption
9. Holding a clear value to the users, apart from privacy enhancement.
10. Countering the bad reputation some 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 PET-tool can become more positive.

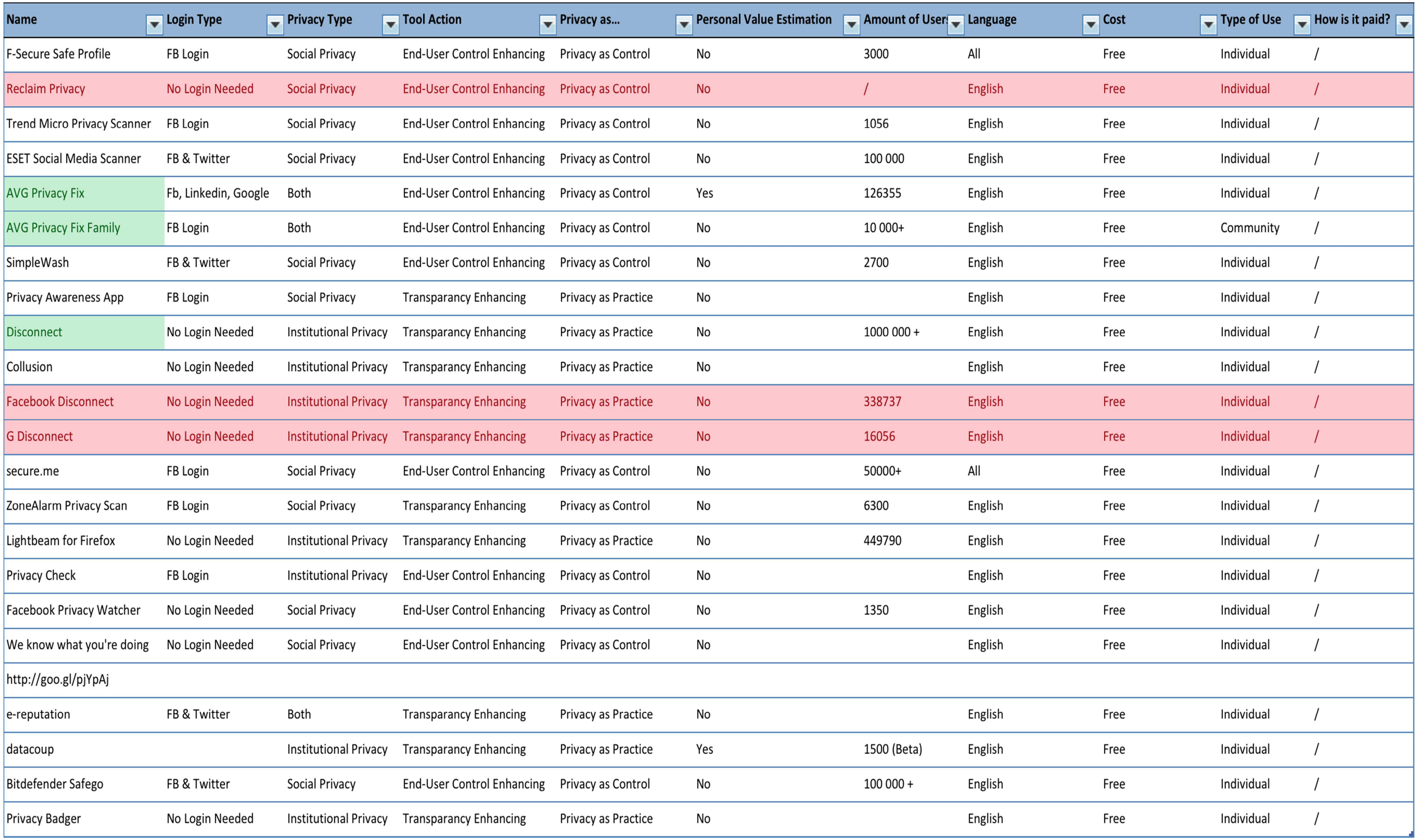
The next logical steps for our research would see how feasible each of these social requirements are and if they lay in the scope of the USEMP project.

8. Annex

8.1. PFA Analysis

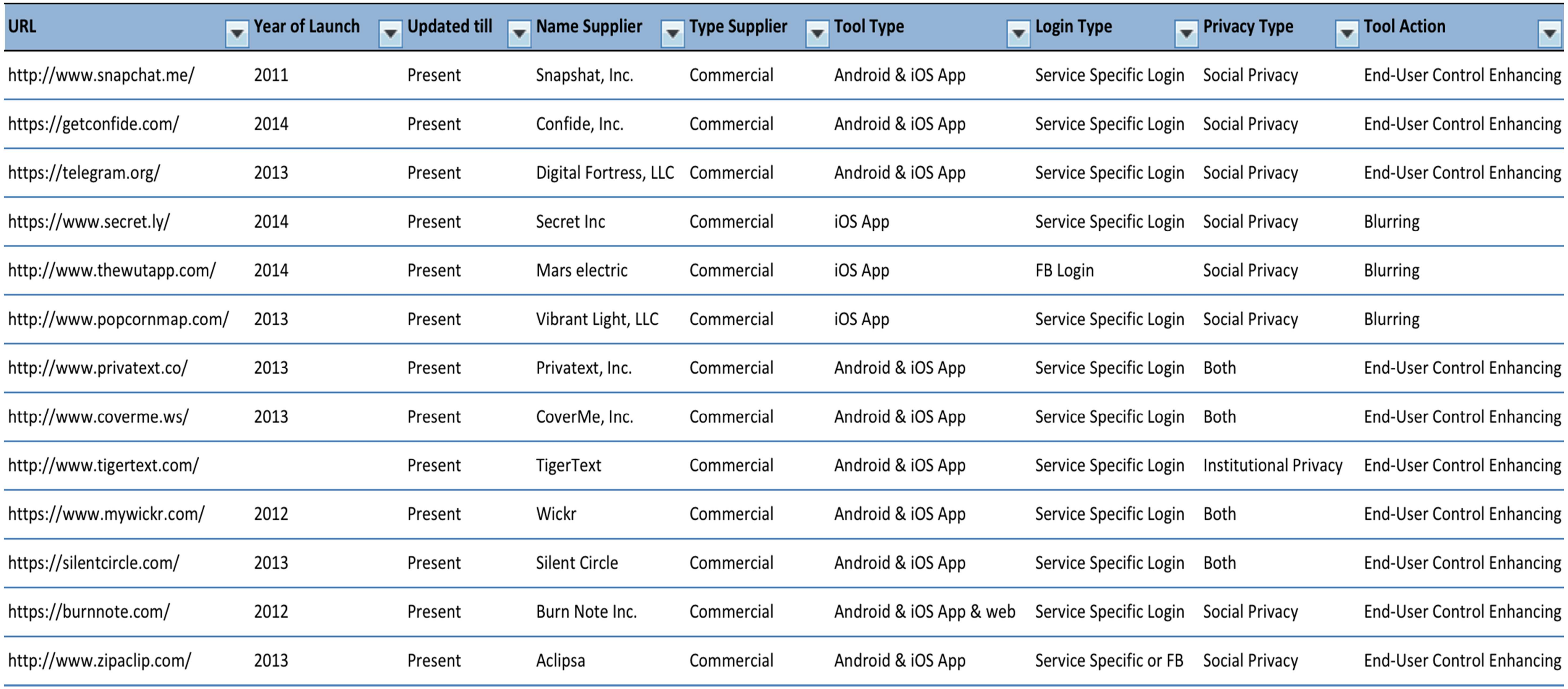


Name	URL	Year of Launch	Updated till	Name Supplier	Type Supplier	Tool Type
F-Secure Safe Profile	https://safeprofile-tp.sp.f-secure.com/	2013	Present	F-Secure	Commercial	Facebook App
Reclaim Privacy	http://www.reclaimprivacy.org/	2010	2011	Volunteers	Individual	Browser Plug-in
Trend Micro Privacy Scanner	https://play.google.com/store/apps/details?id=com.trendmicro.socialprivacyscanner	2013	Present	Trend Micro	Commercial	Android App
ESET Social Media Scanner	https://socialmediascanner.eset.com/	2013	Present	ESET	Commercial	Facebook App
AVG Privacy Fix	https://www.privacyfix.com/start/install	2013	Present	AVG	Commercial	Browser Plug-in
AVG Privacy Fix Family	https://privacyfix.com/Family/index	2014	Present	AVG	Commercial	Facebook App
SimpleWash	http://simplewa.sh/login	2013	Present	While True Labs, LLC	Commercial	Facebook App
Privacy Awareness App	http://www.privacy-awareness-app.org/		Present	WU Vienna Univ	Research	Facebook App
Disconnect	https://disconnect.me/	2011	Present	Disconnect	Commercial	Browser Plug-in
Collusion	https://blog.disconnect.me/collusion-for-chrome	2012	Present	Disconnect	Commercial	Browser Plug-in
Facebook Disconnect	https://chrome.google.com/webstore/detail/facebook-disconnect/ejpepffjfmamnambagiibghpglaidiec	2010	Present	Disconnect	Commercial	Browser Plug-in
G Disconnect	https://chrome.google.com/webstore/detail/g-disconnect/kglfocodeikakacbeoajjhnplhlaoook	2011	Present	Disconnect	Commercial	Browser Plug-in
secure.me	http://www.secure.me/en/	2012	Present	Avast	Commercial	Facebook App
ZoneAlarm Privacy Scan	https://www.facebook.com/appcenter/sgprivacy?fb_source=search&fbsid=1101&fref=ts	2013	Present	Zone Labs, LLC	Commercial	Facebook App
Lightbeam for Firefox	https://addons.mozilla.org/en-US/firefox/addon/lightbeam/	2013	Present	Atul Varma	Research	Browser Plug-in
Privacy Check	http://www.rabidgremlin.com/fbprivacy/		Present	Rabid Gremlin	Individual	Facebook App
Facebook Privacy Watcher	http://www.daniel-puscher.de/fpw/index.php		Present	CASED & TU Darmstadt	Research	Browser Plug-in
We know what you're doing	http://weknowwhatyouredoing.com/	2012	Present	Callum Haywood	Individual	
http://goo.gl/pjYpAj						
e-reputation	http://ereputation.paris.fr/	2014	Present	Paris et MAIF	Other	
datacoup	https://datacoup.com/	2014	Present	datacoup	Commercial	
Bitdefender Safego	http://www.bitdefender.com/solutions/bitdefender-safego.html	2011	2013	Bitdefender	Commercial	Facebook App
Privacy Badger	https://www.eff.org/privacybadger	2014	Present	EFF	Commercial	Browser Plug-in

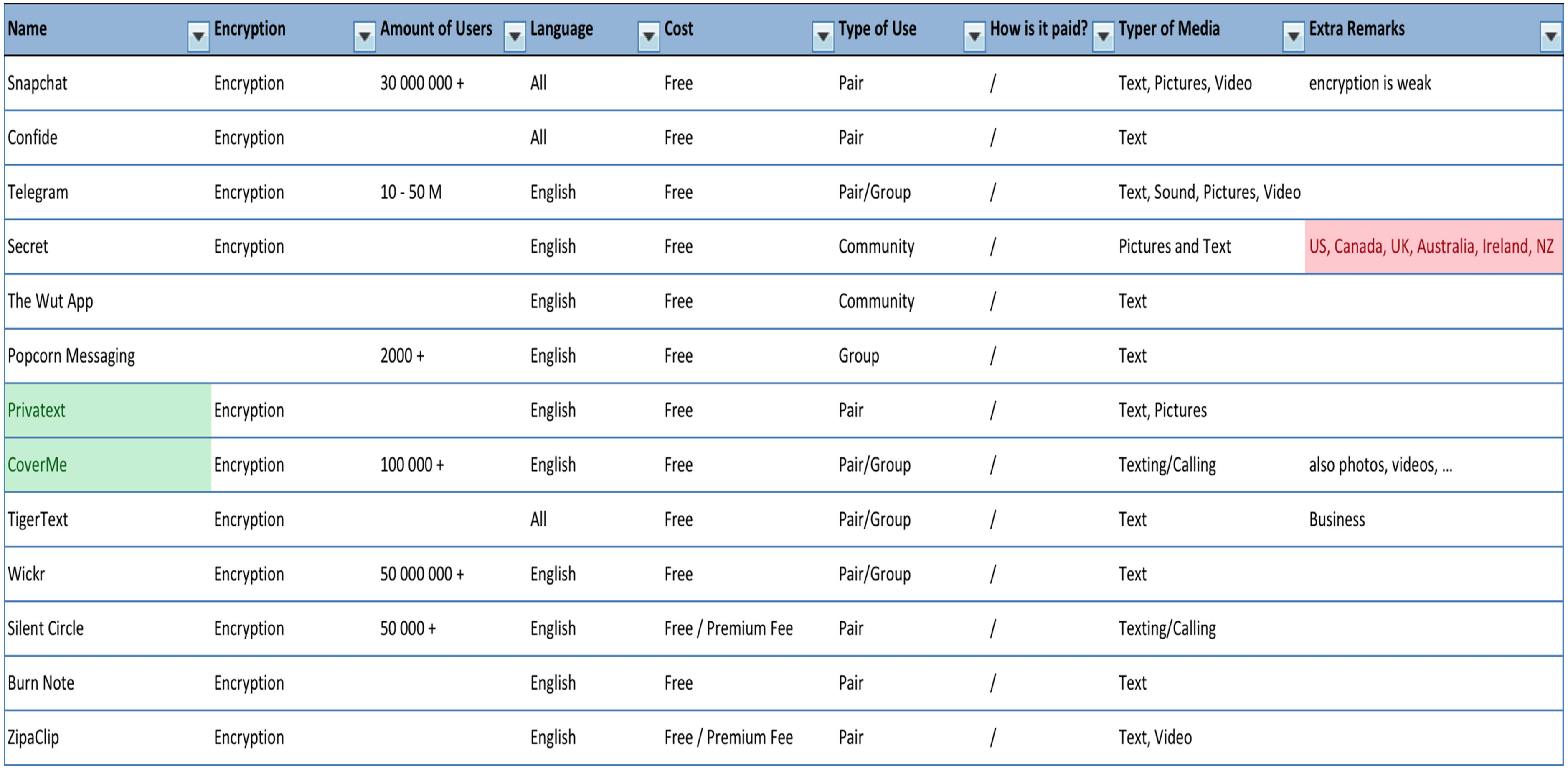


Name	Login Type	Privacy Type	Tool Action	Privacy as...	Personal Value Estimation	Amount of Users	Language	Cost	Type of Use	How is it paid?
F-Secure Safe Profile	FB Login	Social Privacy	End-User Control Enhancing	Privacy as Control	No	3000	All	Free	Individual	/
Reclaim Privacy	No Login Needed	Social Privacy	End-User Control Enhancing	Privacy as Control	No	/	English	Free	Individual	/
Trend Micro Privacy Scanner	FB Login	Social Privacy	End-User Control Enhancing	Privacy as Control	No	1056	English	Free	Individual	/
ESET Social Media Scanner	FB & Twitter	Social Privacy	End-User Control Enhancing	Privacy as Control	No	100 000	English	Free	Individual	/
AVG Privacy Fix	Fb, Linkedin, Google	Both	End-User Control Enhancing	Privacy as Control	Yes	126355	English	Free	Individual	/
AVG Privacy Fix Family	FB Login	Both	End-User Control Enhancing	Privacy as Control	No	10 000+	English	Free	Community	/
SimpleWash	FB & Twitter	Social Privacy	End-User Control Enhancing	Privacy as Control	No	2700	English	Free	Individual	/
Privacy Awareness App	FB Login	Social Privacy	Transparancy Enhancing	Privacy as Practice	No		English	Free	Individual	/
Disconnect	No Login Needed	Institutional Privacy	Transparancy Enhancing	Privacy as Practice	No	1000 000 +	English	Free	Individual	/
Collusion	No Login Needed	Institutional Privacy	Transparancy Enhancing	Privacy as Practice	No		English	Free	Individual	/
Facebook Disconnect	No Login Needed	Institutional Privacy	Transparancy Enhancing	Privacy as Practice	No	338737	English	Free	Individual	/
G Disconnect	No Login Needed	Institutional Privacy	Transparancy Enhancing	Privacy as Practice	No	16056	English	Free	Individual	/
secure.me	FB Login	Social Privacy	End-User Control Enhancing	Privacy as Control	No	50000+	All	Free	Individual	/
ZoneAlarm Privacy Scan	FB Login	Social Privacy	Transparancy Enhancing	Privacy as Control	No	6300	English	Free	Individual	/
Lightbeam for Firefox	No Login Needed	Institutional Privacy	Transparancy Enhancing	Privacy as Practice	No	449790	English	Free	Individual	/
Privacy Check	FB Login	Institutional Privacy	End-User Control Enhancing	Privacy as Control	No		English	Free	Individual	/
Facebook Privacy Watcher	No Login Needed	Social Privacy	End-User Control Enhancing	Privacy as Control	No	1350	English	Free	Individual	/
We know what you're doing	No Login Needed	Social Privacy	End-User Control Enhancing	Privacy as Control	No		English	Free	Individual	/
http://goo.gl/pjYpAj										
e-reputation	FB & Twitter	Both	Transparancy Enhancing	Privacy as Practice	No		English	Free	Individual	/
datacoup		Institutional Privacy	Transparancy Enhancing	Privacy as Practice	Yes	1500 (Beta)	English	Free	Individual	/
Bitdefender Safego	FB & Twitter	Social Privacy	End-User Control Enhancing	Privacy as Control	No	100 000 +	English	Free	Individual	/
Privacy Badger	No Login Needed	Institutional Privacy	Transparancy Enhancing	Privacy as Practice	No		English	Free	Individual	/

8.2. TMT Analysis



URL	Year of Launch	Updated till	Name Supplier	Type Supplier	Tool Type	Login Type	Privacy Type	Tool Action
http://www.snapchat.me/	2011	Present	Snapshat, Inc.	Commercial	Android & iOS App	Service Specific Login	Social Privacy	End-User Control Enhancing
https://getconfide.com/	2014	Present	Confide, Inc.	Commercial	Android & iOS App	Service Specific Login	Social Privacy	End-User Control Enhancing
https://telegram.org/	2013	Present	Digital Fortress, LLC	Commercial	Android & iOS App	Service Specific Login	Social Privacy	End-User Control Enhancing
https://www.secret.ly/	2014	Present	Secret Inc	Commercial	iOS App	Service Specific Login	Social Privacy	Blurring
http://www.thewutapp.com/	2014	Present	Mars electric	Commercial	iOS App	FB Login	Social Privacy	Blurring
http://www.popcornmap.com/	2013	Present	Vibrant Light, LLC	Commercial	iOS App	Service Specific Login	Social Privacy	Blurring
http://www.privatext.co/	2013	Present	Privatext, Inc.	Commercial	Android & iOS App	Service Specific Login	Both	End-User Control Enhancing
http://www.coverme.ws/	2013	Present	CoverMe, Inc.	Commercial	Android & iOS App	Service Specific Login	Both	End-User Control Enhancing
http://www.tigertext.com/		Present	TigerText	Commercial	Android & iOS App	Service Specific Login	Institutional Privacy	End-User Control Enhancing
https://www.mywickr.com/	2012	Present	Wickr	Commercial	Android & iOS App	Service Specific Login	Both	End-User Control Enhancing
https://silentcircle.com/	2013	Present	Silent Circle	Commercial	Android & iOS App	Service Specific Login	Both	End-User Control Enhancing
https://burnnote.com/	2012	Present	Burn Note Inc.	Commercial	Android & iOS App & web	Service Specific Login	Social Privacy	End-User Control Enhancing
http://www.zipaclip.com/	2013	Present	Aclipsa	Commercial	Android & iOS App	Service Specific or FB	Social Privacy	End-User Control Enhancing



Name	Encryption	Amount of Users	Language	Cost	Type of Use	How is it paid?	Typer of Media	Extra Remarks
Snapchat	Encryption	30 000 000 +	All	Free	Pair	/	Text, Pictures, Video	encryption is weak
Confide	Encryption		All	Free	Pair	/	Text	
Telegram	Encryption	10 - 50 M	English	Free	Pair/Group	/	Text, Sound, Pictures, Video	
Secret	Encryption		English	Free	Community	/	Pictures and Text	US, Canada, UK, Australia, Ireland, NZ
The Wut App			English	Free	Community	/	Text	
Popcorn Messaging		2000 +	English	Free	Group	/	Text	
Privatext	Encryption		English	Free	Pair	/	Text, Pictures	
CoverMe	Encryption	100 000 +	English	Free	Pair/Group	/	Texting/Calling	also photos, videos, ...
TigerText	Encryption		All	Free	Pair/Group	/	Text	Business
Wickr	Encryption	50 000 000 +	English	Free	Pair/Group	/	Text	
Silent Circle	Encryption	50 000 +	English	Free / Premium Fee	Pair	/	Texting/Calling	
Burn Note	Encryption		English	Free	Pair	/	Text	
ZipaClip	Encryption		English	Free / Premium Fee	Pair	/	Text, Video	

8.3. Questionnaire Survey

Part 1: Background information

First we would like to ask you some questions about who you are. This is important for us in our analysis of the results

All information is handled with great confidentiality

What is your gender ?

○ Male
○ Female
○ Other

What is your year of birth?

○ After 1998
○ 1998
○ 1997
○ 1996
○ 1995
○ 1994
○ 1993
○ 1992
○ 1991
○ 1990
○ 1989
○ 1988
○ 1987
○ 1986
○ 1985
○ 1984
○ 1983
○ 1982
○ 1981
○ 1980
○ 1979
○ 1978
○ 1977
○ 1976
○ 1975
○ 1974
○ 1973
○ 1972
○ 1971
○ 1970
○ 1969
○ 1968
○ 1967
○ 1966
○ 1965
○ 1964
○ 1963
○ 1962
○ 1961
○ 1960
○ 1959
○ 1958
○ 1957
○ 1956
○ 1955
○ 1954

○ 1953
○ 1952
○ 1951
○ 1950
○ 1949
○ 1948
○ Before 1948

Please indicate below which devices you own (select all relevant)

□ Smartphone (an advanced cell phone for surfing, checking emails, using applications, etc. E.g.: iPhone, Samsung Galaxy, ...)
□ A tablet computer (e.g.: iPad, Samsung Galaxy Tab, Asus Transformer, Microsoft Surface, ...)
□ A desktop
□ A portable computer (e.g. laptop, netbook, ...)
□ A mobile phone (only for making calls or texting)
□ None of the above

Do you use social media ? (E.g. Facebook, LinkedIn, Twitter, etc.)

○ Yes
○ No

Have you ever used privacy enhancing tools? (All sort of tools that you have used to keep your personal information more private on the internet)

○ Yes
○ No
○ I don't know

Please indicate the extent to which you agree on following statements:

______ I usually trust a person until there is a reason not to.
______ Even when the stakes are high, I still think that most people are honest in their dealings with others.
______ In general, people do not really care about the well-being of others.
______ I generally give people the benefit of the doubt when I first meet them.

Please indicate the extent to which you agree on following statements:

	Strongly Disagree	Disagree	Somewhat Disagree	Neither Agree nor Disagree	Somewhat Agree	Agree	Strongly Agree
I am interested in reading political commentaries or watching them on TV.	❍	❍	❍	❍	❍	❍	❍
I closely follow developments in my community.	❍	❍	❍	❍	❍	❍	❍
I enjoy discussing important social issues with others.	❍	❍	❍	❍	❍	❍	❍
I closely follow government regulation of high-tech business (such as information technologies, telecommunications, ...)	❍	❍	❍	❍	❍	❍	❍
I read at least one newspaper (on paper or digital) every day.	❍	❍	❍	❍	❍	❍	❍
I watch news and other television programs/channels that address current issues.	❍	❍	❍	❍	❍	❍	❍

Part 2: Your opinion about privacy on the internet

Please indicate the extent to which you agreeon following statements:

	Strongly Disagree	Disagree	Somewhat Disagree	Neither Agree nor Disagree	Somewhat Agree	Agree	Strongly Agree
All things considered, the internet causes serious privacy problems.	❍	❍	❍	❍	❍	❍	❍
Compared to others, I am more sensitive about the way online companies handle my personal information.	❍	❍	❍	❍	❍	❍	❍
To me, it is the most important thing to keep my privacy intact from online companies.	❍	❍	❍	❍	❍	❍	❍
I believe other people are too much concerned with online privacy issues.	❍	❍	❍	❍	❍	❍	❍
Compared with other subjects on my mind, personal privacy is very important.	❍	❍	❍	❍	❍	❍	❍
I am concerned about threats to my personal privacy	❍	❍	❍	❍	❍	❍	❍

today.							

Please indicate the extent to which you trustthe following entities:

______ Online Stores (e.g. Amazon, Bol.com, ...)
______ Online Social Networks (e.g. Facebook, Twitter, ...)
______ Professional Online Networks (e.g. LinkedIn, XING, ...)
______ Online governmental services (e.g. Tax-on-web, ...)
______ Online banking (e.g. KBC online, ...)
______ Online health services
______ Online review sites (e.g. Tripadvisor, Yelp ...)

When interacting with a web site, I look for ...

	Never	Very rarely	Rarely	Sometimes	Often	Almost always	Always
information about the reputation of the organization.	❍	❍	❍	❍	❍	❍	❍
information about the (physical) location of the organization.	❍	❍	❍	❍	❍	❍	❍
information about the laws that are applicable with regard to my interaction with the organization.	❍	❍	❍	❍	❍	❍	❍
any guarantees regarding confidentiality of the information that I provide.	❍	❍	❍	❍	❍	❍	❍
information about the complaint procedures in case of problems.	❍	❍	❍	❍	❍	❍	❍
information about who is liable in case of problems.	❍	❍	❍	❍	❍	❍	❍
trust marks or seals of approval (such as McAfee Secure, TRUSTe, ...)	❍	❍	❍	❍	❍	❍	❍

When using an online application, I'm able ...

	Strongly Disagree	Disagree	Somewhat Disagree	Neither Agree nor Disagree	Somewhat Agree	Agree	Strongly Agree
to understand my rights and duties as described by the Terms of the application provider.	❍	❍	❍	❍	❍	❍	❍
to detect when my personal information has been misused.	❍	❍	❍	❍	❍	❍	❍
to detect when a third party has gained access to the application without authorization.	❍	❍	❍	❍	❍	❍	❍
to assess the effectiveness of available redress mechanisms to remedy any problems or harms.	❍	❍	❍	❍	❍	❍	❍

Part 3: Internet Use

When you are using the internet, how often do you...

	Never	Less than Once a Month	Once a Month	2-3 Times a Month	Once a Week	2-3 Times a Week	Daily
save files	❍	❍	❍	❍	❍	❍	❍
use the refresh button	❍	❍	❍	❍	❍	❍	❍
upload files, so you can also access them from a different computer.	❍	❍	❍	❍	❍	❍	❍
download programs	❍	❍	❍	❍	❍	❍	❍
watch video files	❍	❍	❍	❍	❍	❍	❍
find web sites to be confusing	❍	❍	❍	❍	❍	❍	❍
get lost	❍	❍	❍	❍	❍	❍	❍
feel disoriented	❍	❍	❍	❍	❍	❍	❍
experience difficulties with a web site's layout	❍	❍	❍	❍	❍	❍	❍
not know where you are	❍	❍	❍	❍	❍	❍	❍
check information retrieved on another web site	❍	❍	❍	❍	❍	❍	❍
examine only the top results	❍	❍	❍	❍	❍	❍	❍
find the information you were looking for	❍	❍	❍	❍	❍	❍	❍
examine the results on subsequent result	❍	❍	❍	❍	❍	❍	❍

pages							
use more than one search keyword	❍	❍	❍	❍	❍	❍	❍
make a decision based on retrieved information	❍	❍	❍	❍	❍	❍	❍
use information about a specific subject from multiple sites	❍	❍	❍	❍	❍	❍	❍
benefit from using the internet	❍	❍	❍	❍	❍	❍	❍
use reference web sites (e.g. Wikipedia, Yahoo! Answers, About.com, ...)	❍	❍	❍	❍	❍	❍	❍
gain financial benefits	❍	❍	❍	❍	❍	❍	❍

Part 4: Social Media Use

Which types of web 2.0 websites have you used in the last month? (Select all relevant)

❑ Social networking, e.g. Facebook, LinkedIn
❑ Photo sharing, e.g. Instagram, Flickr
❑ Micro blogging, e.g. Twitter, Plurk
❑ Conversation apps, e.g. WhatsApp, Skype
❑ Self destruction messages, e.g. Snapchat, Wickr
❑ Music, e.g. last.fm, Google Music
❑ Publishing, e.g. SlideShare
❑ Video, e.g. YouTube, Vine, Viddler
❑ Location-based social networks (e.g. Foursquare, Find my friends, ...)
❑ Crowdcreation, e.g. Amazon mechanical turk, Innocentive, iStockPhoto
❑ Crowdvoting, e.g. Threadless, Tricider
❑ Crowdwisdom, e.g. Wikipedia, Idea jams
❑ Crowdfunding, e.g. Kiva, Micro-loans
❑ Virtual worlds, e.g. Second Life
❑ Massively multiplayer online game, e.g. World of Warcraft
❑ None of the above
❑ Other, namely ____________________

Do you use Facebook?

❍ Yes
❍ No

Answer If Do you use Facebook? Yes Is Selected

Please indicate the extent to which you agree on the following statements about your Facebook use :

	Strongly Disagree	Disagree	Somewhat Disagree	Neither Agree nor Disagree	Somewhat Agree	Agree	Strongly Agree
I make use of private communication channels (e.g. Facebook chat) when I want to talk about sensitive subjects.	❍	❍	❍	❍	❍	❍	❍
I review photos friends tag me in before they appear on my timeline.	❍	❍	❍	❍	❍	❍	❍
I make sure that only friends can see my profile.	❍	❍	❍	❍	❍	❍	❍
I only post information on Facebook that is suitable for everyone that can see it.	❍	❍	❍	❍	❍	❍	❍
I untag myself from photos I don’t find appropriate.	❍	❍	❍	❍	❍	❍	❍
When I install an application on Facebook, I make sure that I am the only one who can see this.	❍	❍	❍	❍	❍	❍	❍
I don’t fill in all the information that is requested by Facebook.	❍	❍	❍	❍	❍	❍	❍
I am careful from who I accept friend requests.	❍	❍	❍	❍	❍	❍	❍
I make use of	❍	❍	❍	❍	❍	❍	❍

Facebook lists when posting information.							
I defriend those I no longer want to see my status updates.	❍	❍	❍	❍	❍	❍	❍

Please indicate how often you do the below actions when using social media:

	Never	Very rarely	Rarely	Sometimes	Often	Almost always	Always
I adjust privacy settings when I use social media	❍	❍	❍	❍	❍	❍	❍
I use fake personal information (contact information, age, ...) when I use online services	❍	❍	❍	❍	❍	❍	❍
I ask somebody (friends, parents, etc.) what I should do to protect my data on the internet	❍	❍	❍	❍	❍	❍	❍
I read the privacy statements of the website before entering my personal information	❍	❍	❍	❍	❍	❍	❍
When I have to enter my personal information on a website, I go to another, similar website that doesn't require this information.	❍	❍	❍	❍	❍	❍	❍
I provide incomplete information about me when I	❍	❍	❍	❍	❍	❍	❍

register on a website							

Please indicate the extent to which you agree on following statements:

	Strongly Disagree	Disagree	Somewhat Disagree	Neither Agree nor Disagree	Somewhat Agree	Agree	Strongly Agree
I am often concerned that I don't have control over the actions of other users.	❍	❍	❍	❍	❍	❍	❍
It bothers me when other users tag me in pictures.	❍	❍	❍	❍	❍	❍	❍
It bothers me when other users post something about me on their wall.	❍	❍	❍	❍	❍	❍	❍

Part 5: Privacy Tool Use

Below a few questions regarding your usage of privacy enhancing tools. These tools are used in different devices (e.g. smartphone, PC, etc.) to make your personal information less exposed throughout the internet.

Are you aware of the existence of tools that can help protect your data online?

○ Yes, and I have used them before
○ Yes, but I have not used them before
○ No

Answer If Are you aware of the existence of tools that can help protect your data online? Yes, and I have used them before Is Selected Or Are you aware of the existence of tools that can help protect your data online? Yes, but I have not used them before Is Selected

Which privacy tools do you use and/or have you heard of?

	I have used	I have heard	I haven't used nor heard
Financing, e.g. Bitcoin, Litecoins	❍	❍	❍
File erasing programs, e.g. Eraser	❍	❍	❍
Anonymous e-mails, e.g. Guerillamail	❍	❍	❍
E-mail encryption, e.g. enigmail	❍	❍	❍
Anonymous search engine, e.g. DuckDuckGo	❍	❍	❍
Anonymous browser, e.g. Onion browser	❍	❍	❍
Anonymous remailers, e.g. Quicksilver, Micmaster	❍	❍	❍
Encryption of files, e.g. TrueCrypt	❍	❍	❍
Password vaults, e.g. Passwordsafe, 1password	❍	❍	❍
Secure instant messaging, e.g. BlackSMS, Cryptocat	❍	❍	❍
Cookie/cache/internet history cleansers, e.g. CCleaner	❍	❍	❍
Publishing, e.g. Media crush, pastebin	❍	❍	❍
Private social networks, e.g. Diaspora, Movin	❍	❍	❍
Encrypted voice/video, e.g. Linphone, Mumble	❍	❍	❍
VPN accounts, e.g. Autistici/Inventati, TOR	❍	❍	❍

Answer If Which privacy tools do you use and/or have you heard of? (select all relevant actions) - I have used Is Greater Than or Equal to 1

How do you rate your current state of protection after using these tools combined together?

○ Very Dissatisfied
○ Dissatisfied
○ Neutral
○ Satisfied
○ Very Satisfied

Answer If Which privacy tools do you use and/or have you heard of?&nbsp; - I have used Is Greater Than or Equal to 1

Do you believe these tools that you use are enough to protect your privacy?

○ Yes
○ No
○ I don't know

Answer If Which privacy tools do you use and/or have you heard of?&nbsp; - I have used Is Equal to 0

If you have not used any of these tools, why not?

○ I am not aware of them
○ I am not sure if I need one
○ I don't believe my privacy is at risk
○ I think they are too complex too work with
○ Other reason, namely ____________________

Final Part: Privacy Feedback and Awareness (PFA) Tool use

Privacy Feedback and Awareness (PFA) tools are used to inform the user about a breach of privacy over the internet. They can have several formats such as apps within an online social network (e.g. FB Safe profile), as an add-on to a browser (e.g. Disconnect), etc.

Are you aware of PFA tools?

○ Yes, and I have used them before
○ Yes, but I have not used them before
○ No

Answer If Are you aware of PFA tools? Yes, and I have used them before Is Selected Or Are you aware of PFA tools? Yes, but I have not used them before Is Selected

What privacy tools have you heard and/or used of?

	I have used this tool	I have heard of this tool	I haven't used nor heard of this tool
FB Safe Profile	○	○	○
Reclaim Privacy	○	○	○
Trend Micro Privacy Scanner	○	○	○
ESET Social Media Scanner	○	○	○
AVG Privacy Fix	○	○	○
AVG Privacy Fix Family	○	○	○
SimpleWash	○	○	○
Privacy Awareness App	○	○	○
Disconnect	○	○	○
Secure.me	○	○	○
ZoneAlarm Privacy Scan	○	○	○
Lightbeam for Firefox	○	○	○
Privacy Check	○	○	○
Bitdefender Safego	○	○	○

Answer If What privacy tools have you heard and/or used of? - I have used this tool Is Greater Than or Equal to 1

How do you rate your current state of protection after using these tools in general?

○ Very Dissatisfied
○ Dissatisfied
○ Neutral
○ Satisfied
○ Very Satisfied

Answer If What privacy tools have you heard and/or used of? - I have used this tool Is Greater Than or Equal to 1

Do you believe these tools that you use are enough to protect your privacy?

○ Yes
○ No
○ I don't know

Answer If What privacy tools have you heard and/or used of? - I have used this tool Is Equal to 0

If you have not used any of these tools, what is the reason?

○ I am not aware of them
○ I am not sure if I need one
○ I don't believe my privacy is at risk
○ I think they are too complicated to work with
○ Other reason, namely ____________________

8.4. Topic Guide Focus group sessions (in Dutch)

8.4.1. Structuur

a) Inleiding: Voorstelling moderatoren, regels focusgroep (5")
b) Tijdsplanning meedelen (5")
c) Informed Consent laten ondertekenen + Schaal laten invullen (10")
d) Voorstelling deelnemers + ijsbreker (10")
e) Van algemeen naar Privacy & Technologie (10")
f) Privacy online (20")
g) Economie achter het delen van informatie (20")
h) Privacy enhancing tools (25")
   a. Kennis
   b. Voorstellen + laten vallen dat je mensen nodig hebt om gebruik te testen
   c. Oefening: de ideale tool
i) Afsluiten + Uitnodiging gebruik tool (10")
j) Kort kaderen onderzoek USEMP (5")

8.4.2. Inleiding: Voorstellen moderatoren + regels focus group (5")

- Voorstellen moderator/co-moderator
  - Wijzen op broodjes en drank
  - Wijzen op opnameapparatuur: uitleggen waarom, gesprekken worden nadien verwijderd, personen geanonimiseerd. Ok? Opname starten.
- Regels focusgroep:
  - Inzicht krijgen in voorkeuren, waarden, meningen
  - Laat jullie gedachten maar de vrije loop
  - Geen juist/fout
  - 1 persoon praat tegelijkertijd: belangrijk voor de opname

8.4.3. Tijdsplanning meedelen (5")

8.4.4. Informed Consent laten ondertekenen + schalen laten invullen (10")

Bij de schalen ook wat extra informatie vragen: naam deelnemers, geboortedatum, emailadres (belangrijk voor wie wilt meewerken aan vervolg onderzoek)

8.4.5. Voorstellen deelnemers + ijsbreker (10")

- Naam
- Leeftijd
- Beroep
- Interesses
- Motivatie voor deelname
- ijsbreker: Kan je je een moment voor de geest halen wanneer je het gevoel had dat jouw privacy geschonden werd/informatie over jou online stond dat je liever niet had gewild

8.4.6. Van algemeen naar Privacy & Technologie (10”)

- Wat betekent privacy voor jou?
- In welke mate denk je na over het onderwerp?
- Wordt er in je sociale kring vaak over gepraat? Wanneer? Zijn er mensen waar je dit meer mee doet dan anderen?

- Hoe kunnen nieuwe technologieën een effect hebben op je privacy?
- Wat is voor jullie het belangrijkste verschil tussen offline en online privacy?
-
- Wanneer je een nieuwe technologie gaat gebruiken, hou je dan op voorhand rekening met de gevolgen voor je privacy? (Kosten/baten-afweging, vb. Sociale Media)

8.4.7. Privacy Online (20”)

Filmpje: https://www.youtube.com/watch?v=BgE4JpeDGR8

- Hoeveel informatie denk je dat je dagelijks deelt online?
- Op welke manieren denk je dat het internet gevolgen heeft voor je privacy of de veiligheid van je persoonlijke data?

Slide met de verschillende vormen van persoonlijke data tonen

- Denk je aan specifieke websites/bedrijven die dit soort data verzamelen?
- Weet je hoeveel informatie je over jezelf deelt? Pas je hier bewust voor op?
- Wat is voor jou de belangrijkste reden om je privacy te beschermen? Denk je dat je dit te weinig doet? Waarom? Wat zou je aanzetten om dit wel te doen?

Korte oefening: Welke strategieën gebruik je om je privacy te beschermen online

Op papier even de tijd geven om neer te schrijven

- **Vb’n**: niet op sociale media, bepaalde informatie bewust niet delen, privacy settings aanpassen, bepaalde informatie slechts met een aantal mensen delen, gevoelige informatie via de chat, doelbewust gebruiken van valse persoonlijke informatie, PETs, …)

8.4.8. Economie achter het delen van informative (20”)

Filmpje: http://www.een.be/programmas/koppen/digitaal-goud

Niet volledig: enkel deel over internet privacy, kort om dit te schetsen

- Wat vind je van wat je net gezien hebt?
- Heeft dit je verbaasd? Was je op de hoogte dat sociale netwerken je informatie gebruiken om je advertenties op maat te geven?
- Heb je het gevoel dat je je hiertegen kan beschermen?

- In het filmpje zagen we ook iets over bedrijven die volgen naar welke sites je surft en wat je opzoekt.
- Wat vind je hiervan?
- Wat kan wel/niet door de beugel?
- Doen jullie hier iets tegen? Wat zou je hier tegen willen doen?
- Wie is verantwoordelijk voor het beschermen van de gebruiker? (beschermingsmaatregelen vanuit de gebruiker, OSNs, bedrijven, overheid?)

8.4.9. Middelen om je privacy te beschermen (25”)

- Wist je dat er bepaalde software, plugins, applicaties bestaan die je persoonlijke data online helpen beschermen?
- Wat weet je hiervan?
- Welke zijn bekend voor jou?
- Heb je er al aan gedacht om zo’n tools te gebruiken? Gebruik je ze reeds? Waarom niet?/zou je zoiets willen gebruiken?

Ik zou jullie 3 bestaande tools even willen laten zien: Ghostery/PrivacyBadger/AVG Privacy Fix/PrivacyBadger

Tijdens het tonen even uitleggen wat ze doen, na elke tool:

- Wat vind je hiervan?
- Zou dit iets zijn dat je zou gebruiken? Waarom wel? Wat houdt je tegen?
- Wat is voor jou het belangrijkste zodat je zo’n tool zou gebruiken?
- Wat zou je tegenhouden? Zie je er iets negatief aan?

Oefening: de ideale tool

Als je iets aan de voorgestelde tools zou willen veranderen? Hoe ziet jouw ideale PET eruit, waarom en wanneer zou je hem gebruiken?

8.4.10. Afsluiten van de focus group + uitnodiging herhalen gebruik tool

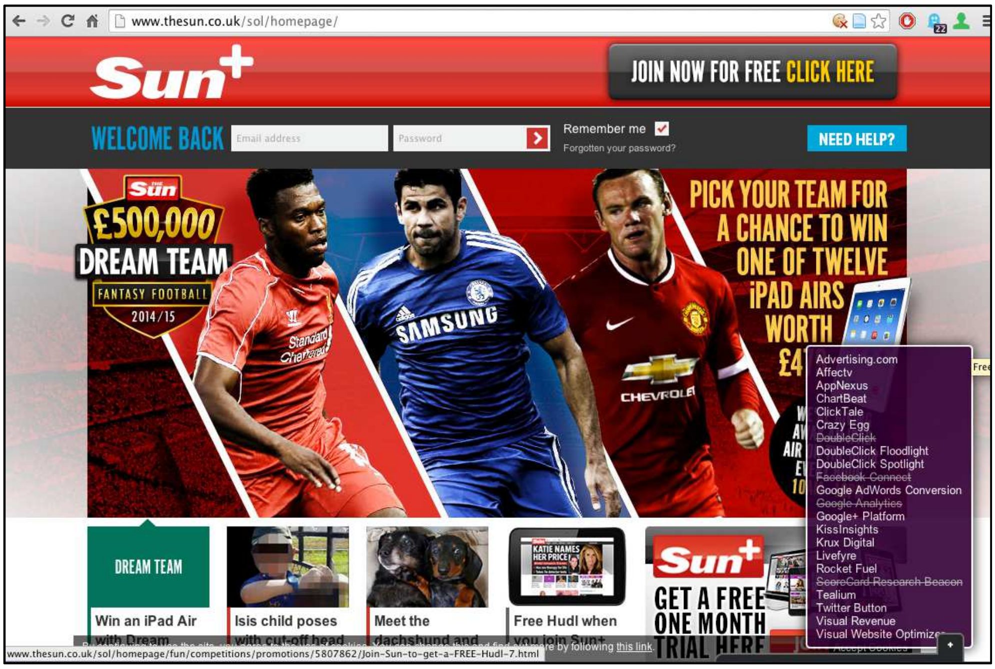
Willen jullie nog iets kwijt? Is er nog iets dat je niet kon zeggen tijdens de focusgroep?

8.5. Focus group privacy tools: Ghostery and AVG Privacy Fix

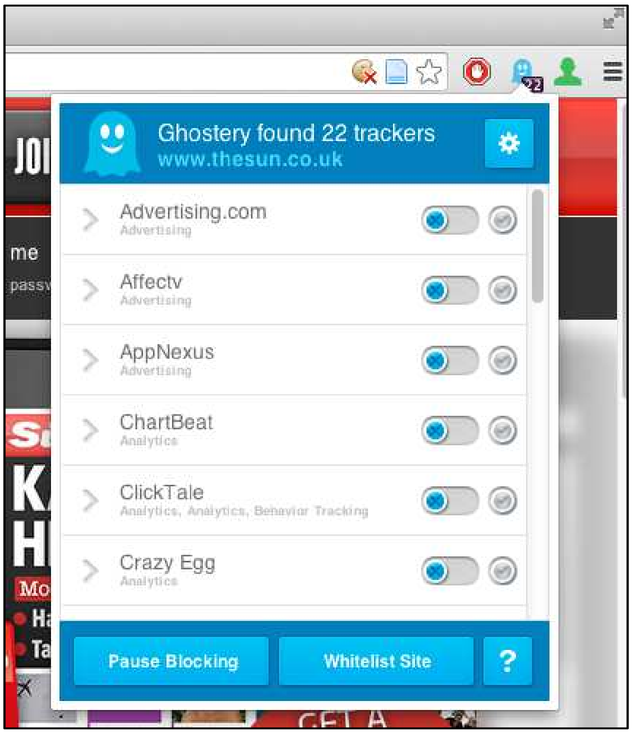
8.5.1. Ghostery

The main features of Ghostery include:

1. Showing which data brokers are following you on every website.
2. Providing the ability to turn off the different trackers individually
3. The user can get more information about the trackers privacy policy, which data is collected and with whom it is shared.

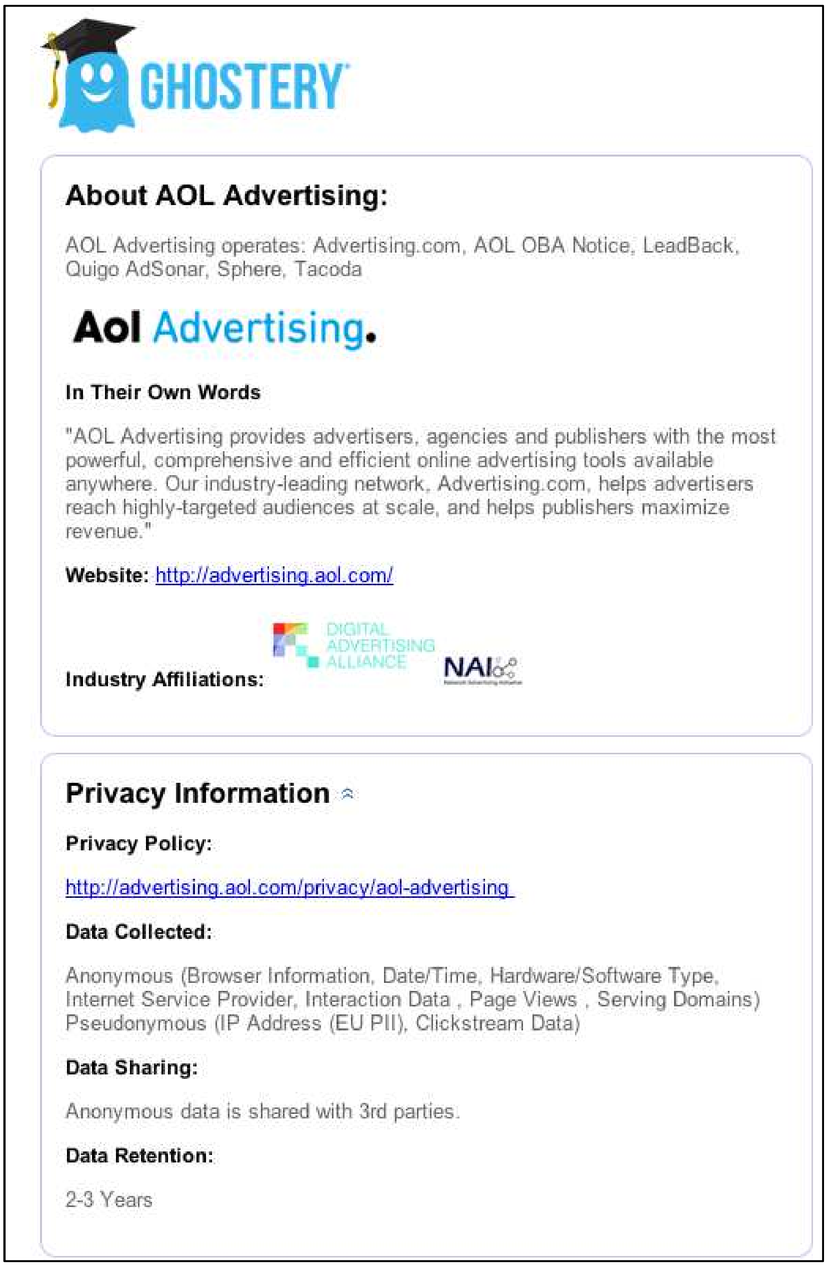

www.thesun.co.uk/sol/homepage/
Sun+
JOIN NOW FOR FREE CLICK HERE
WELCOME BACK
Email address
Password
Remember me
Forgotten your password?
NEED HELP?
Sun £500,000 DREAM TEAM FANTASY FOOTBALL 2014/15
PICK YOUR TEAM FOR A CHANCE TO WIN ONE OF TWELVE iPAD AIRS WORTH £4
DREAM TEAM
Win an iPad Air with Dream
Isis child poses with cut-off head
Meet the dachshund and
Free Hudl when you join Sun+
Sun+ GET A FREE ONE MONTH TRIAL HERE
www.thesun.co.uk/sol/homepage/fun/competitions/promotions/5807862/Join-Sun-to-get-a-FREE-Hudl-7.html

Advertising.com
Affectv
AppNexus
ChartBeat
ClickTale
Crazy Egg
~~DoubleClick~~
DoubleClick Floodlight
DoubleClick Spotlight
~~Facebook Connect~~
Google AdWords Conversion
~~Google Analytics~~
Google+ Platform
KissInsights
Krux Digital
Livefyre
Rocket Fuel
~~ScoreCard Research Beacon~~
Tealium
Twitter Button
Visual Revenue
Visual Website Optimizer



Ghostery found 22 trackers
www.thesun.co.uk

Advertising.com	Advertising
Affectv	Advertising
AppNexus	Advertising
ChartBeat	Analytics
ClickTale	Analytics, Analytics, Behavior Tracking
Crazy Egg	Analytics



About AOL Advertising:

AOL Advertising operates: Advertising.com, AOL OBA Notice, LeadBack, Quigo AdSonar, Sphere, Tacoda

In Their Own Words

"AOL Advertising provides advertisers, agencies and publishers with the most powerful, comprehensive and efficient online advertising tools available anywhere. Our industry-leading network, Advertising.com, helps advertisers reach highly-targeted audiences at scale, and helps publishers maximize revenue."

Website: http://advertising.aol.com/

Industry Affiliations:

Privacy Information

Privacy Policy:

http://advertising.aol.com/privacy/aol-advertising

Data Collected:

Anonymous (Browser Information, Date/Time, Hardware/Software Type, Internet Service Provider, Interaction Data , Page Views , Serving Domains) Pseudonymous (IP Address (EU PII), Clickstream Data)

Data Sharing:

Anonymous data is shared with 3rd parties.

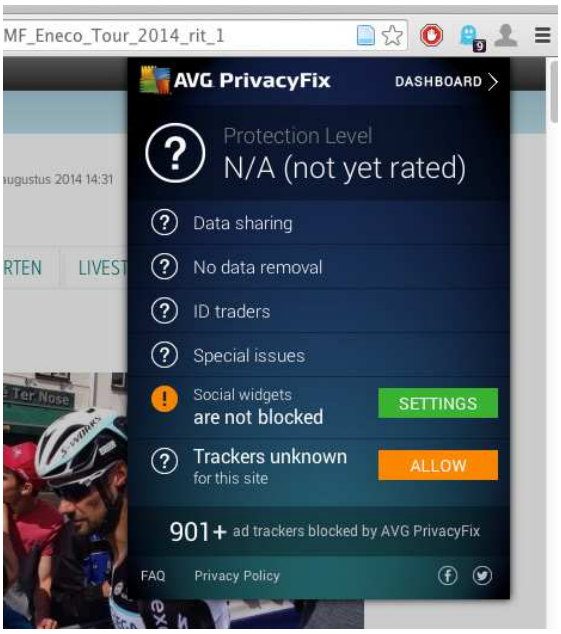
Data Retention:

2-3 Years

8.5.2. AVG Privacy Fix

The main features of AVG Privacy Fix include:

1. A short overview of the privacy policy of the site a user visits is presented
2. It blocks advertising trackers
3. It shows an estimation of the value of your data to Google
4. It offers the possibility to help you change your privacy settings on LinkedIn and Twitter


MF_Eneco_Tour_2014_rit_1

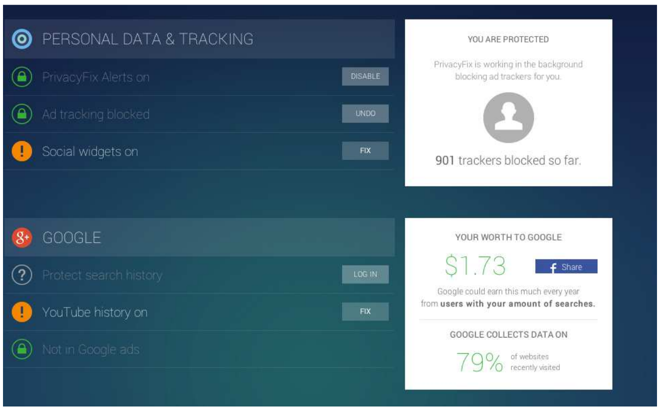
AVG PrivacyFix DASHBOARD

Protection Level
N/A (not yet rated)

- Data sharing
- No data removal
- ID traders
- Special issues
- Social widgets are not blocked SETTINGS
- Trackers unknown for this site ALLOW

901+ ad trackers blocked by AVG PrivacyFix

FAQ Privacy Policy


PERSONAL DATA & TRACKING

- PrivacyFix Alerts on DISABLE
- Ad tracking blocked UNDO
- Social widgets on FIX

YOU ARE PROTECTED

PrivacyFix is working in the background blocking ad trackers for you.

901 trackers blocked so far.

GOOGLE

- Protect search history LOG IN
- YouTube history on FIX
- Not in Google ads

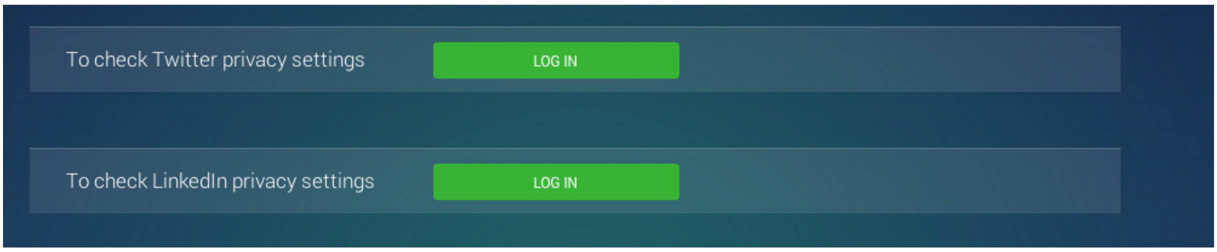
YOUR WORTH TO GOOGLE

$1.73 Share

Google could earn this much every year from **users with your amount of searches.**

GOOGLE COLLECTS DATA ON

79% of websites recently visited


To check Twitter privacy settings LOG IN

To check LinkedIn privacy settings LOG IN

8.6. Informed Consent Focus group Sessions (in Dutch)

GEÏNFORMEERDE TOESTEMMING STUDIE

U hebt beslist dat u wil deelnemen aan een onderzoekssessie georganiseerd door iMinds-SMIT, VUB, waarvoor onze dank! In dit document zetten we alle informatie aangaande deze studie nog eens op een rijtje. Nadat u deze informatie hebt doorgenomen, kan u onderaan uw deelname bevestigen.

Situering van de sessie

De sessie maakt deel uit van een onderzoeksproject waarbinnen wordt onderzocht hoe gebruikers meer controle kunnen uitoefenen op hun persoonlijke data op het internet. Sociaal-wetenschappelijk en technologisch onderzoek vullen elkaar hierbij aan. De feedback die we van u tijdens deze sessie verzamelen is voor ons uiterst belangrijk om verdere technologische ontwikkelingen te sturen vanuit een menselijk oogpunt.

USEMP betreft een interdisciplinair project, waaraan zowel academische als industriële onderzoekspartners deelnemen. Het project wordt gesubsidieerd door de Europese Commissie in het kader van het Seventh Framework Programme for Research (FP7).

Invulling sessie

Tijdens de sessie peilen we naar uw mening over privacy en proberen we een inzicht te verkrijgen in uw opinie over het delen van persoonlijke informatie online. De sessie is eenmalig en duurt maximaal 2 uur.

Vertrouwelijke behandeling van uw gegevens

De inzichten van deze sessie worden ter beschikking gesteld van de partners binnen het project en kunnen door hen gebruikt worden. De ruwe audiogegevens die tijdens het onderzoek worden verzameld, worden niet doorgegeven aan derden, binnen noch buiten het project. Bij rapportering van de resultaten van het onderzoek aan derden, blijven de deelnemers aan het onderzoek steeds anoniem.

Door het ondertekenen van dit document, verklaart u op de hoogte te zijn van de aard van het onderzoek en bereid te zijn hier aan deel te nemen.

Voor akkoord namens uzelf,

.... (datum) Naam en handtekening:

Voor akkoord namens iMinds,

.... (datum) Naam en handtekening:

9.Bibliography

Alessandro Acquisti and Jens Grossklags (2005) Privacy and Rationality in Individual Decision Making, *IEEE Security and Privacy*, IEEE Computer Society, Vol. 3, No. 1, January/February 2005, pp. 26-33.

Barnes, S.B. (2006). A privacy paradox: Social networking in the United States. First Monday, 11(9).

Boyd, danah and Alice Marwick. 2011. “Social Steganography: Privacy in Networked Publics.” Paper presented at ICA on May 28, 2011 in Boston, MA. http://www.danah.org/papers/2011/Steganography-ICAVersion.pdf

Brandtzæg, P.B., Lüders, M., & Skjetne, J.H. (2010). Too many Facebook "Friends"? Content Sharing and Sociability Versus the Need for Privacy in Social Network Sites. *Journal of Human-Computer Interaction,* 26(11-12), 1006-1030

Bryman, A. (2012). *Social Research Methods*. Oxford University Press.

Deuker, A. (2010). Addressing the privacy paradox by expanded privacy awareness–the example of context-aware services. In *Privacy and Identity Management for Life* (pp. 275–283). Springer. Retrieved from http://link.springer.com/chapter/10.1007/978-3-642-14282-6_23

Diaz, C., & Gürses, S. (2012). Understanding the landscape of privacy technologies. *Extended Abstract of Invited Talk in Proceedings of the Information Security Summit*, 58–63.

Duysburgh, P., & Jacobs, A. (2010). Collaboration through ICT between Healthcare Professionals: The Social Requirements of Health 2.0 Applications. In *Electronic Healthcare* (pp. 165–172). Springer. Retrieved from http://link.springer.com/chapter/10.1007/978-3-642-11745-9_26

Gürses, S. (2011). D2. 2-Requirements and Conceptual Framework. *Information Privacy*, *53*, 1393–1462.

Gürses, S., & Diaz, C. (2013). Two Tales of Privacy in Online Social Networks. *Security & Privacy, IEEE*, *11*(3), 29–37.

Hendrik, J. G. O., Sunday, O. O., & Oludayo, O. O. (2013). A PET Evaluation Framework for Relational Databases (pp. 612–617). IEEE. doi:10.1109/SocialCom.2013.92

Krasnova, H., Günther, O., Spiekermann, S., & Koroleva, K. (2009). Privacy concerns and identity in online social networks. *Identity in the Information Society*, *2*(1), 39–63. doi:10.1007/s12394-009-0019-1

Norberg, P. A., Horne, D. R., & Horne, D. A. (2007). The privacy paradox: Personal information disclosure intentions versus behaviors. *Journal of Consumer Affairs*, *41*(1), 100–126.

Pierson, J. (2012). Online privacy in social media: A conceptual exploration of empowerment and vulnerability. *Communications & Strategies*, *4*(88), 99–120.

Pötzsch, S. (2009). Privacy awareness: A means to solve the privacy paradox? In *The Future of Identity in the Information Society* (pp. 226–236). Springer. Retrieved from http://link.springer.com/chapter/10.1007/978-3-642-03315-5_17

Raynes-Goldie, K. (2010) ‘Aliases, creeping, and wall cleaning: understanding privacy in the age of Facebook’, First Monday, vol. 15, no. 1, [Online] Available at: http://firstmonday.org/htbin/cgiwrap/bin/ojs/index.php/fm/article/view/2775/2432 (15 March 2011).

Smith, H., Milberg, S., & Burke, S. (1996). Information Privacy: Measuring Individuals’ Concerns about Organizational Practices. *Management Information Systems Quarterly*, *20*(2). Retrieved from http://aisel.aisnet.org/misq/vol20/iss2/3

Taddicken, M. (2014). The “Privacy Paradox” in the Social Web: The Impact of Privacy Concerns, Individual Characteristics, and the Perceived Social Relevance on Different Forms of Self-Disclosure. *Journal of Computer-Mediated Communication*, *19*(2), 248–273. doi:10.1111/jcc4.12052

Van Dijck, J. (2011). Flickr and the culture of connectivity: Sharing views, experiences, memories. *Memory Studies*, *4*(4). doi:10.1177/1750698010385215

Van Dijck, J. (2013). *The Culture of Connectivity: A Critical History of Social Media*. Oxford University Press.

Young, A. L., & Quan-Haase, A. (2013). Privacy Protection Strategies on Facebook: The Internet privacy paradox revisited. *Information, Communication & Society*, *16*(4), 479–500. doi:10.1080/1369118X.2013.777757

Zimmerman, Mark A. & Rappaport, Julian (1988). Citizen participation, perceived control and psychological empowerment. American Journal of Community Psychology, 16, 725-743