Utrecht University
Master psychology, Applied Cognitive Psychology

THESIS

Privacy Dashboards: Control and Understanding of Data through Usability and User Experience

S.I. van Gogh, 3968596
June 30, 2017

Supervisor UU
dr. J.S. Benjamins

Supervisor TNO
T. Wabeke

Second Assessor UU
dr. S.M. Stuit

Abstract

With the rising trend of big data, activity trackers, and dashboards, privacy is more important than ever. In this thesis, an intuitive way was researched for the user to understand and control his data in dashboards. This was done in two steps. The first step encapsulated the design expectations of the user by means of a questionnaire about usability, privacy, and data sharing. The results indicate that a user's understanding of what happens to his data is more important than having control over said data. The second step was the making of a design, a prototype, and eventually the implementation, of privacy settings in a dashboard. This implementation was evaluated in a field test. Although the results must be taken with caution, because of the limited number of respondents, the results suggest that the implemented design was user-friendly. Even though both steps combined form no conclusive result, they indicate that the design may serve as a basis for future research. More research should be done to confirm these indications.

Acknowledgements

First and foremost, I would like to thank my supervisors Thymen Wabeke (TNO) and dr. Jeroen Benjamins (UU), who always made time for me whenever I had questions or troubles regarding data, writing or anything else.

I would also like to thank Ir. Ward Venrooij for his cooperation on the designs and his inexhaustible source of enthusiasm for my work and this project as a whole.

Next, I would also like to thank all my fellow interns and colleagues, who made it a pleasure to travel to Den Haag or Soesterberg, and, at times, have helped me with my problems on both a professional and a personal level.

I would also like to acknowledge everyone who participated in either the first questionnaire that was conducted or the trial in which the implementation of the design was evaluated. Without them, this thesis would not have been possible.

Finally, I would like to thank Paul van Gogh, Nathalie Korbee, and Joost de Vries for proofreading and commenting on my thesis whenever I asked for it. Your input and suggestions were invaluable and very much appreciated.

Thank you.
Stef van Gogh

Table of Contents

1 Introduction

There has been a steady increase in the number of smartphones users in the Netherlands, from 56% of the total population in 2012 to almost 85% in 2016 (Centraal Bureau voor de Statistiek, 2016c), most of which are Android-based (IDC, 2016). Furthermore, the number of Android apps alone has increased by a factor of 163: from 16,000 in 2009 to 2,600,000 in 2016 (Statista, 2016). Most of these apps aim to improve the life of the smartphone user, but apps can, at the same time, also be used to track your every move. In the documentary "Addicted to my phone" (3Doc, 2016), a team of Danish researchers and programmers developed a flashlight app with the same permissions as the Facebook app, and showed the possible consequences of all of these permissions. They were, for instance, able to turn on the microphone and record conversations without the smartphone user's knowledge, take photos, and scroll through all photos and text messages. In the end, the researchers used the GPS location of the users to drive to their house and confront them with the collected data. As expected, many users reacted shocked and appalled by this confrontation, because they believed that all of their data was private.

This is an example of data collection without the user's knowledge. This is a problem, because there is a trend towards online information, such as dashboards for private information (see Figure 1). It is important for the user to have insight in his data, and that the privacy of the user is not violated. In this section, the core concepts of the abovementioned problem will be explained, namely *privacy*, *trust*, and *usability*. Finally, the concept of dashboards will be explained. This section ends with the research questions that this thesis looks to answer.

One of the reasons that the users of the flashlight app were so appalled, can be that humans want to be able to choose which data to share and when (Westin, 2003). While human minds can change between different states of privacy—sometimes sharing private information with complete strangers and sometimes with close friends—the important factor is that the individual can choose when to share and what to share. The protection of data is required by EU law (EU Directive, 1995), but the collection of all this data by Facebook or any other app is, so far, legal. The protection of data is even more important when talking about private or medical information. Sankar et al. (2003) explain that patients are reluctant to share private information, because they do not trust what happens with their private data. Even though patients might be reluctant to share their information, they are still more motivated to share sensitive information than healthy people (Grande et al., 2015; Truven Health Analytics, 2015). Furthermore, Zukowski & Brown (2007) found a correlation between privacy concerns and age, and between privacy concerns and level of education. Younger people and higher educated people are less worried about their online privacy.

Who gets to read the personal information is important too. Lederer et al. (2003) found that the 'who' is more important than the situation. If the 'who' is not trusted, then personal data will not be shared under any circumstances. For example, if patients do not trust their doctors, they will not share their personal information with them. Or rather, if employees do not trust their manager, they will not share their personal information with him or her. This, of course, boils down to the principle of trust in an individual or an organization. Trust is defined by Fogg et al. (1999) as: *"A positive belief about the perceived reliability of, dependability of, and confidence in a person, object, or process."*. This suggests that privacy and trust are closely related, and that trust is a very important factor in sharing personal data.

Studies also suggest that usability and trust are closely related, especially online (Bedi & Banati, 2006; Sasse, 2005). Specifically, Roy et al. (2001) found that four out of five usability factors increase the trust in websites: *ease of navigation*, *ease of learning*, *perception* and *support*, while *consistency* was the only factor that did not appear to make an impact on trust. In other words, the more user-friendly the website is, the more the user will trust it. Yoon (2002) states that trust and website satisfaction are strongly related, although they do respond differently to trust antecedents, and Kim & Moon (1998) found that it is possible to induce feelings of e.g., trustworthiness by manipulating visual design factors of the customer interface.

When a website is easier to use, users are more likely to return to that website. Cheskin Research & Studio Archetype/Sapient (1999) modeled trust in 3 stages. Trust begins in a state

of chaos, this happens when users enter a website for the first time. Users desire to gain control in an unknown situation. Especially if this situation requests the use of personal information. This is when people build trust at an extrinsic level. Extrinsic trust factors are defined by Jøsang et al. (2005) as *"information elements that are communicated between parties"*. The second stage is reassurance of their worries, like controlling their personal information. This gives users a sense of online security. Seals of Approval (e.g., Visa or PayPal) can build trust in this phase. Here, users rely on both extrinsic and intrinsic trust. Intrinsic trust factors are explained by Jøsang et al. (2005) as *"information elements emerging from personal experience"*. The third and last stage is maintaining the trust level. At this stage, visitors pay more attention to usability and user experience (UX) (Nielsen & Norman, 2000). This is also the stage that visitors solely rely on intrinsic trust factors (Yoon, 2002). This suggests that usability and UX are responsible for building trust and helps people develop a sense of loyalty to the website.

Dashboards

Companies can collect staggering amounts of data. This data can be used to steer organizations. For example, a manager can make informed decisions when looking at customer satisfaction levels or sales per product. However, this data is usually too much or too cluttered when looking at an excel sheet. To show these large amounts of data, a concept was developed in the early 1980s: dashboards (Few, 2006). Dashboards had a slow start in the early stages, but since the upcoming Big Data scene, dashboards are widely used around the world. For example, every website that uses Google Analytics has a dashboard, as this is a standard feature. A dashboard is defined by Few (2004) as:

> *"a visual display of the most important information needed to achieve one or more objectives; consolidated and arranged on a single screen so the information can be monitored at a glance."*

While dashboards used to be only for businesses, it starts to become a trend in every day life too. An example of this is the trend in actigraphy (sleeptrackers, etc.). For instance, Microsoft has its own version of the well-known FitBit called the Microsoft Band. This tracks your steps, sleep, workouts, and much more. All of this data can be seen online in a dashboard[1]. However, not everyone is willing to share this data, so something must be done to protect their data.

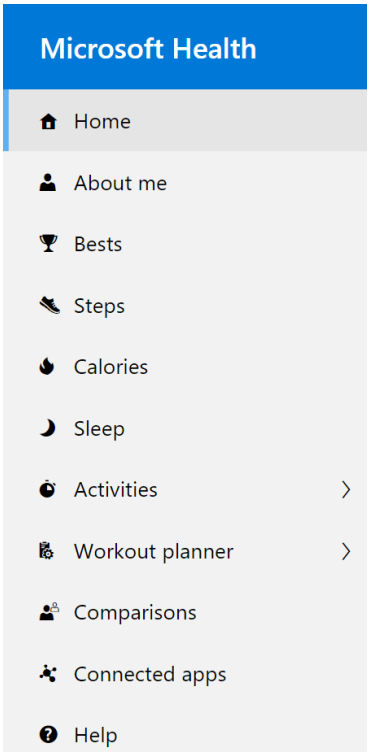


Figure 1: Menu in the Microsoft Health dashboard. Privacy settings are not intuitively accessible.

The ultimate goal is to increase the users' trust in what happens to their data. By giving the user more control and insight in his or her personal (health care) data in an intuitive way, the trust in the system should increase (Phelps et al., 2000). To obtain this goal, a relatively new type of dashboard has been made: the 'Privacy Dashboard'. These privacy dashboards are meant to provide the user with a clear and intuitive overview of their collected data and to give the user control over the processing or usage of their personal data[2][3] (Zimmermann et al., 2014).

As stated above, usability, trust and privacy are related to each other. However, that does not always mean that big corporations make privacy settings in their (privacy) dashboards easy to find. For example, one could argue that the privacy settings for the Microsoft Band can be found in the Microsoft Health dashboard, the same dashboard in which the Microsoft Band data is shown. All settings can be seen in Figure 1. Surprisingly, no privacy settings were found, so

[1] https://dashboard.microsofthealth.com/
[2] https://account.microsoft.com/privacy
[3] https://www.google.com/dashboard

Microsoft's privacy statement[4] was consulted. The privacy statement states that all personal data can be controlled in the Microsoft privacy dashboard. The option in the privacy dashboard to control private information sends you back to the Microsoft Health dashboard. This is one of many examples where privacy settings can not be found so easily; meanwhile, it is unknown what exactly is happening to the collected data.

It is not only important to be able to find the privacy settings, but also to ensure that the privacy settings are respected and secured throughout the whole application. Therefore, privacy design strategies were invented to support privacy, by designing the system architecture in such a way that it actively supports data privacy. Hoepman (2014) wrote an article on these privacy design strategies, in which he explains eight strategies. The focus in this thesis is on the strategies that involve the users: 'Inform' and 'Control'. The 'Inform' strategy is one that focuses to *inform* the users how personal data is processed. The 'Control' strategy focuses on giving the user *control* over the processing of their personal data.

To combine the control and inform strategies in privacy dashboards with the aforementioned factors, namely trust and usability, this thesis focuses on the following questions:

RQ1 How can users be informed intuitively about the use of their personal data in a privacy dashboard?

RQ2 How can a privacy dashboard be designed in a way that it helps the user understand what happens to his data and how the user can control this?

In conclusion, some research has been done on the technical side of privacy dashboards (see also Zimmermann et al. (2014)), but hardly any research on the cognitive design aspects of privacy dashboards. The scope of this thesis is to contribute to this shortcoming.

In this thesis a couple of steps were taken in order to reach the above mentioned objective. First, a questionnaire regarding privacy and usability was conducted. A prototype was made using the results of this questionnaire. The prototype was evaluated by peers and TNO employees. Eventually the prototype was implemented and subjected to a field test to see if the prototype was, in fact, intuitive to use. The results of the test are expected to be positive, with which a recommendation or discouragement can be made about certain design choices for future projects.

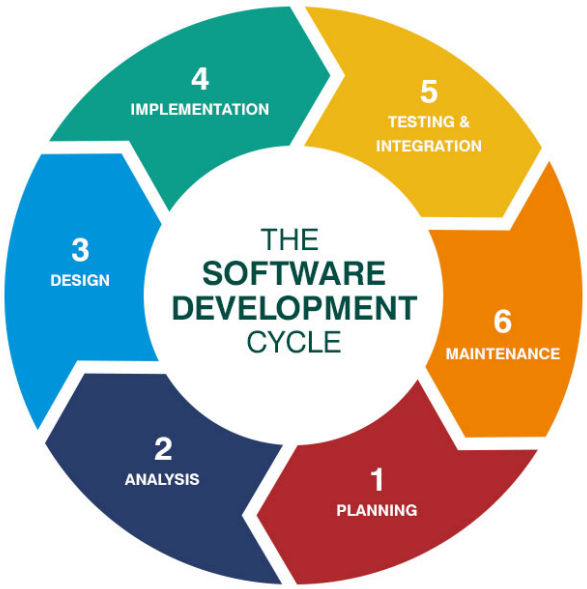


Figure 2: The software development life cycle. Each cycle ends with a release. The next iteration of the cycle uses the last release as its starting point.

[4] https://privacy.microsoft.com/en-us/privacystatement

2 Methods

Since this is a field test of actual software, the process—including the questionnaire and field test—will be described using the Software Development Life Cycle.

In (software) projects, the development of software is split in phases according to the Software Development Life Cycle (SDLC), which can be seen in Figure 2. The SDLC can be used on different levels, both on a top level (e.g., a project as a whole), and a low level, (e.g., an improvement or repairing a software bug). In both cases the cycle functions more like a guide than as strict rules to follow.

2.1 Planning

As can be seen in Figure 2, the first phase of the SDLC is "planning". This phase is also described as the requirements capture phase. In the planning phase, the development team explores what has to be built and sets up use cases.

In this phase, potential users were involved to help clarify the requirements for the design. This was done by by means of the aforementioned questionnaire, so that many people could be reached and the threshold for participating would be very low. The questionnaire took approximately 10 minutes to complete. The full questionnaire can be found in Appendix A.

The questionnaire was distributed via a personal account on social media, namely Facebook and WhatsApp, and email. The questionnaire was set up in such a way that it was made difficult to participate more than once (i.e. only once per device), however, this was not monitored in any way.

Social media was chosen for the distribution of the questionnaire, as this is a very powerful tool to reach many people in a short period of time. Social media also allows resharing by respondents, reaching different demographic groups. The downside of this, is that the population is not a random selection and may be biased.

The questionnaire consisted of 28 questions in total. These were divided into the following sections:

- basic demographics: age, education, gender;
- privacy in hypothetical scenarios;
- usability of hypothetical designs;
- attitude towards sharing private data with others.

The application was developed as a web application, which can be opened on different devices, such as desktop or mobile. This, in turn, raised the question on the popularity of different mobile operating systems for design purposes, as web applications show differently on mobile devices than on desktop.

In the privacy section, respondents of the questionnaire were asked to indicate how important control over their data is, and how important insight is into who can see their data. Next, hypothetical scenarios were presented, and respondents had to choose to what extent their privacy would be violated on a 5-point Likert scale.

In the usability section, a design was shown and respondents were asked to indicate their expectations and wishes on design choices, like placement of functionality, or choice of words.

The last section of the questionnaire gathered information about the attitude towards sharing private data with different people. The private data categories were inspired by previous research (de Vos et al., 2016) in combination with the objective of the current dashboard. This led to the following categories:

1. stress;
2. sleep quality;
3. performance at work;
4. fitness;
5. motivation;
6. absence.

Roles with whom data could be shared with were inspired by (major) roles in the company. The chosen roles are present in most reasonable-sized companies:

1. manager;
2. HR;
3. colleagues;
4. researchers.

For every role and data category combination, respondents were asked to indicate whether they would share that information with that role with one of the following responses: (1) No; (2) Yes, on team level; (3) Yes, individually; and (4) Don't know. Team level meant that data from everyone in the team would be aggregated and, therefore, would not be retraceable to an individual.

Every question was followed by an optional comment box—except for the demographic questions—in which additional feedback could be given by the respondents.

Questions regarding usability and data sharing were not used for statistical analysis, but rather taken into consideration during the design, because the answers are highly subjective. Jacobsen et al. (1999) stated that "*while each user may know what he or she wants, no one can see the whole picture.*".

The results of the questionnaire were analyzed using R v3.3.3. For all statistical analyses a significance level of $\alpha = .05$ was used. Chi-square tests were used to determine any difference between demographic groups within questions, and Wilcoxon signed rank tests were used to determine the differences between different questions. For the latter, questions answered with "Don't know" were excluded, as these can not be given any value on a Likert scale. Other answers were scaled from 1 through 5, where 1 equals "Strongly disagree" and 5 equals "Strongly agree".

The results of this questionnaire were analyzed and used for the design and implementation of the privacy settings. Results of the questionnaire and the discussion can be found in subsection 3.1 and subsection 4.1, respectively.

2.2 Analysis

The second phase of the SDLC (see Figure 2) is "Analysis".

> *"In analysis we analyze the requirements as described in requirements capture by refining and structuring them. The purpose of doing this is to achieve a more precise understanding of requirements and to achieve a description of the requirements that is easy to maintain and that helps us give structure to the whole system—including its architecture."* -Jacobsen et al. (1999, p. 131)

The requirements for the project were already established, but were not explicitly written down. As the project came along, the requirements were incrementally added and accepted into the project. All requirements were in the form of issues on the version control website GitLab[5]. Issues are small increments that focus on improving the software on one specific point (e.g. software bug, new feature, etc.). For the sake of consistency in the project, all requirements for this thesis were added as issues on GitLab, too.

2.3 Design

> *"In design we shape the system and find its form (including its architecture) that lives up to all requirements—including all nonfunctional requirements and other constraints—made on it."* -Jacobsen et al. (1999, p. 215)

To answer research question 2—*how can a privacy dashboard be designed in a way that it helps the user understand what happens to his data and how the user can control this?*—and before starting the implementation of the product, designs have to be made. These designs are the

[5] https://about.gitlab.com/

foundation for the implementation. Design covers both back end and front end development, meaning it can be seen from both a software architectural point of view and an interaction designer point of view. The design for the software architecture was done by the data scientists working on the project. The interaction and screen designs were made by Ward Venrooij and myself.

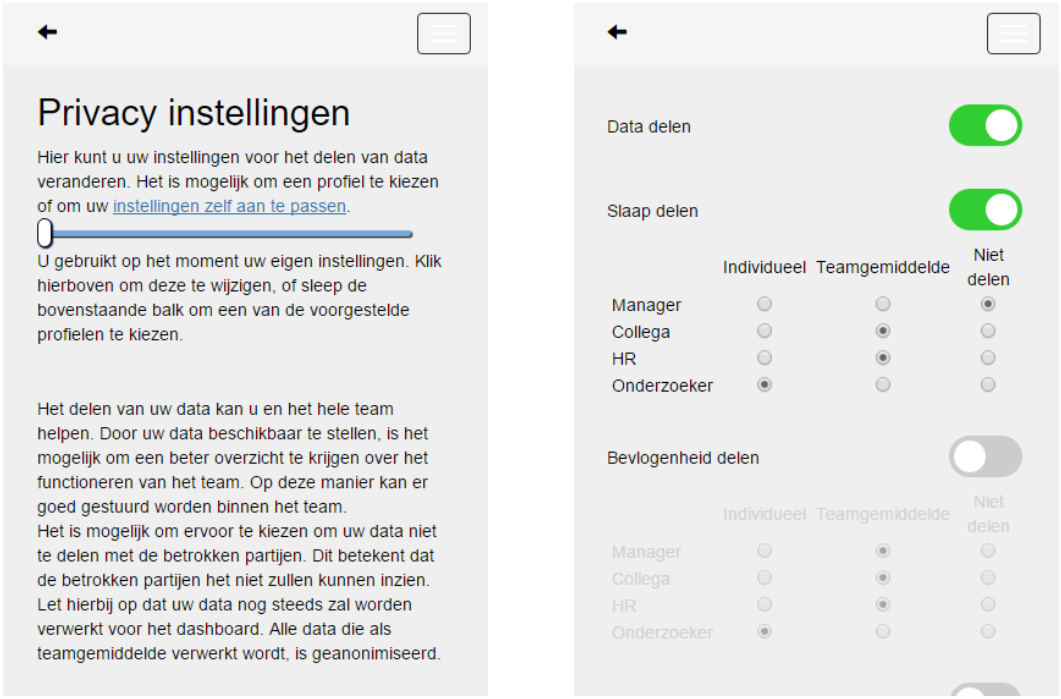
2.3.1 Prototyping

Prototyping is a way of designing, and is usually done in a later stage in the design process, after some ideas and mock-ups are made. The advantage of prototyping, is that prototypes are usually interactive and very low-cost. When prototyping, the design team can make interactive "programs", that solely focus on fixing the problem at hand, without needing the whole application.

A program called "Justinmind"[6] was used as prototyping tool. The program supports mobile, tablet and desktop prototyping, which means that it can simulate how the design would work on a mobile phone, tablet or PC with limited interactions (e.g. clickable features). During the prototyping process, the prototypes were evaluated on the fly by fellow interns, students, and employees. The screen designs can be found in Appendix B and Appendix C.

The privacy settings screen (Appendix B) is provided with a so-called "slider". A slider is an element that collects input within a certain range, and with a certain step interval that the programmer can specify (see Figure 3a). Overall, there were 6 privacy presets to choose from, therefore the range of the slider was $[0-5]$. The text underneath the slider changed whenever the value of slider changed, updating the description to the current privacy preset.

The second screen (Appendix C) is provided with switches per data category and radiobuttons per role. With these elements every category and role can be adjusted to the users exact liking, both on individual level and on data category level.



(a) Privacy settings with slider (blue bar) to adjust privacy preset.

(b) Advanced privacy settings with the ability to control everything on individual level.

Figure 3: Implementation result of the privacy settings pages based on the screen designs.

[6] www.justinmind.com

2.4 Implementation

After the final prototype was accepted by the design team, the next phase in the SDLC (see Figure 2) began: "Implementation".

> "*In implementation, we start with the result from design and implement the system in terms of components, that is, source code, scripts, binaries, executables, and the like.*" -Jacobsen et al., p. 267

During the implementation phase, all prototype screens were converted to code. Using a combination of AngularJS, HTML5, CSS3, jQuery, and plain JavaScript, the screens were implemented over the course of a number of weeks. These frameworks were used, because the privacy settings were added to an existing project, which already used these frameworks. The implementation of both privacy settings screens can be seen in Figure 3. The difference between the screen design (Appendix C) and the implementation (Figure 3b) can be explained by the missing "dimension" in the screen design. The screen designs only accounted for the binary option of sharing or not sharing, which can be done by means of a checkbox. However, it did not take all the options mentioned in subsection 2.1 into account. This was fixed in the implementation by means of a matrix with comboboxes.

When using JavaScript, it can be hard to save settings on a database, because JavaScript is clientside only. The back end was set up in such a way that the application could only receive information, and not send information. Without the ability to send information back, a different approach to save the data must be used. By using browser cookies, the state of the client can be saved on the client side, meaning that the next time they log in, the user will see the screen as if all the settings were saved in a database. One of the problems with this, is that user settings can not be seen and therefore not be analyzed. Web analytics was used to address this problem.

2.4.1 Analytics

Analytics tools can log everything the user does. It collects a considerable amount of data and it can give insights into e.g., usability problems. Most popular analytics tools, like Google Analytics, are very likely to send user logs to their server too, because these services are hosted on their servers. As this project concerns private information, an analytics tool that respects privacy requirements should be used. An alternative to Google Analytics that also takes privacy into account is "Piwik"[7]. Piwik is an open source analytics tool that is installed on your own server. This means that the collected data will not be sent to any third parties, and therefore remains private.

Piwik was implemented using their own JavaScript API[8]. Piwik allows the tracking of custom made events. To log every important action, a piece of code was added to individual actions, such as button presses or changing the slider, and functions that were called for a general action, such as navigating through the application. The code to add a custom made event can be seen in Listing 1.

```
_paq.push(['trackEvent', category, action, name, value]);
```

Listing 1: Piwik tracking code. *Category*, *action*, *name*, and *value* are variable names.

Every button and switch in the advanced privacy settings had these custom events set up. The slider also logged an event any time the value changed, i.e., someone changed the preset privacy settings. For example, when a user changes the privacy preset from setting 1 to setting 2, 1 event would be logged; when he changes it from setting 1 to setting 6, 5 events would be logged (one for each single value change). Piwik logs all (custom made) events, which can be

[7] https://piwik.org/
[8] https://developer.piwik.org/guides/tracking-javascript-guide

monitored in the Piwik dashboard. In the Piwik dashboard, it possible to also filter custom events on *category*, *action*, and *name*.

Piwik also logs the amount of unique visitors to a website. A unique visitor is described by Piwik as "The number of unduplicated visitors coming to your website. Every user is only counted once, even if he visits the website multiple times a day." However, Piwik also states that "When a same person visits your website on two different devices (for example their laptop and on their mobile phone) then Piwik will detect two unique visitors."[9]. Thus, it is important to note that 1 participant can correspond to one or more unique visitor(s), meaning that "visitor" and "participant" are very different. The trial lasted for two weeks, however, due to some limitations of our Piwik implementation, only data for a whole month at a time could be used. Therefore, the data for the month May was used.

Piwik can export the log files in all sorts of ways including, but not limited to, CSV and XML. These file types were imported and analyzed using R v3.3.3. The results and discussion of the analytics can be found in subsection 3.2 and subsection 4.2, respectively.

2.5 Testing & Integration

> *"In the test workflow, we verify the result from implementation by testing each build, including both internal and intermediate builds, as well as final versions of the system to be released to external parties."* -Jacobsen et al. (1999, p. 295)

Every completed issue was manually tested on a local server. This way, the chances of releasing errors became significantly smaller. When everything was ready to be released, another test was conducted to make sure the whole system was working as intended. This test lasted for two weeks and required test participants to use the system as if they were users. All participants were TNO employees. Participants could submit problems to the development team, which in turn would release a fix for that specific problem.

2.6 Maintenance

While maintenance is in the SDLC, it is not part of this project. Maintenance offers no additional benefits for this research and will therefore not be discussed.

2.7 Follow-up Questionnaire

To accommodate the lack of data from web analytics, an extra questionnaire was sent out to the participants to evaluate the privacy settings. The full questionnaire can be found in Appendix D. The questionnaire had 17 questions in total. The questionnaire had some redirection logic in it, meaning that some questions were skipped by respondents, because of the answers given to previous questions. Questions 5–14 are questions from the System Usability Scale (SUS) questionnaire (Brooke, 1996). The questions were directly translated to Dutch.

The SUS questionnaire has its own scoring algorithm to conclude whether a system is user-friendly or not (Brooke, 1996). Bangor et al. (2009) found that with a score of 70 or above, the system is generally found acceptable by the users. Therefore, this study aims for a SUS score of 70 or higher on the implemented designs.

The results and the discussion of the follow-up questionnaire can be found in subsection 3.3 and subsection 4.3, respectively.

3 Results

3.1 Questionnaire

Out of the 152 participants who started the questionnaire, 123 finished it, giving an overall response rate of 81%. The incomplete questionnaires were not taken into consideration. Incom-

[9] https://piwik.org/faq/general/faq_43/

Table 1: Age and gender demographics of respondents. Percentages are rounded to the nearest integer. Most respondents are between 20 and 29 years old.

Age group	0-19	20-29	30-39	40-49	50-59	60+	Total
Male	0% (*0*)	24% (*30*)	5% (*6*)	5% (*6*)	8% (*10*)	2% (*3*)	45% (*55*)
Female	2% (*2*)	30% (*37*)	6% (*7*)	3% (*4*)	9% (*11*)	6% (*7*)	55% (*68*)
Total	2% (*2*)	54% (*67*)	11% (*13*)	8% (*10*)	17% (*21*)	8% (*10*)	100% (*123*)

Values in parentheses are number of respondents

pleteness may have been caused by the fact that it was a Dutch questionnaire being shared over social media. Non-Dutch speakers may have opened the questionnaire and tried to fill it out, resulting in incomplete responses. Other reasons for the partial questionnaires could have been caused by factors such as lack of time.

3.1.1 Demographics

The demographics can be seen in Table 1. Most respondents were in the 20-29 age group (54%). This could have been caused by the way of distribution: social media. The questionnaire was shared mostly in young, academic circles.

Figure 4 shows that 98 out of the 123 respondents (80%) are highly educated (HBO or University). Highly educated people are over-represented in the respondents, as they should only represent 23% of the population (Centraal Bureau voor de Statistiek, 2016b). This can also be explained by social media, because the questionnaire was mostly shared in academic circles.

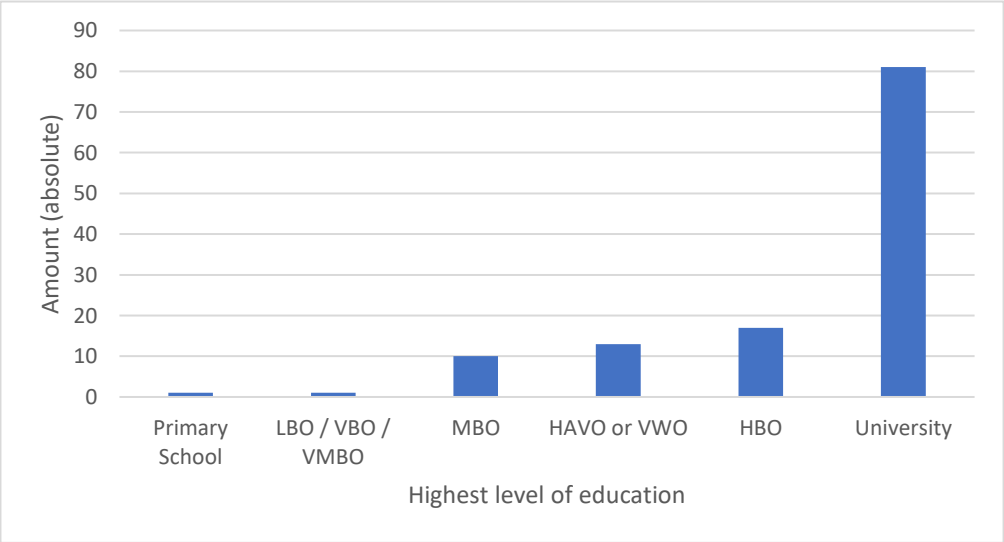


Figure 4: Highest level of education. The x-axis shows the education level; the y-axis shows the amount of respondents (absolute). Most respondents (98 out of 123) have are highly educated: HBO or University.

3.1.2 Privacy

The question "To what extent is it important for you to control your data?" (question 5 in Appendix A), most respondents (around 85%) answered either "important" (56%) or "very important" (29%). To the question "To what extent is it important for you to understand who you share your data with?" (question 7), still around 85% of respondents answered "important" or "very important", but in this case more respondents answered with "very important" (37%). The differences between the two questions can be seen in Figure 5. This could suggest that it is

more important to understand what is happening to your data than it is to control it. However, a Wilcoxon signed rank test indicated that this result is not significant ($p > .05$). Chi-square tests were used to examine any difference between men and women in questions 5 and 7, but again no significant results were found ($p > .05$).

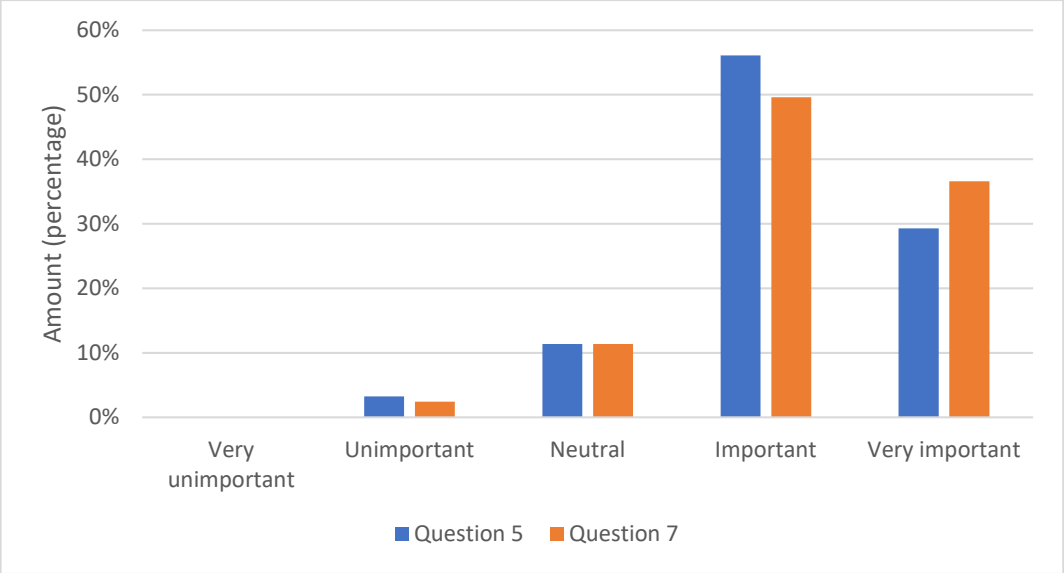


Figure 5: Difference between questions regarding control over sharing your data (blue) and understanding who you share your data with(orange). The question regarding understanding your data has a slight shift towards "very important".

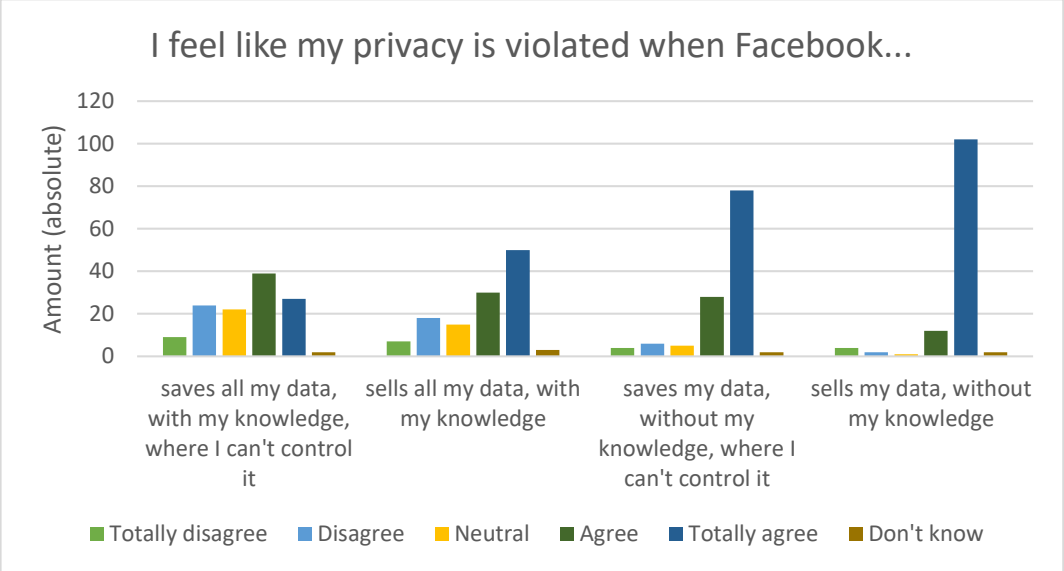


Figure 6: Answers to question 9. The y-axis shows the amount of respondents (absolute). The difference between with or without knowledge can clearly be seen. People feel like their privacy is more violated when they have no knowledge.

Question 9 (see Appendix A, and Figure 6) is about the feeling of violation of privacy. The sub-questions about Facebook storing the data (1st and 3rd) were compared. The only difference between these sub-questions was whether the user has knowledge of the fact that the data is being stored or not. The same was done for the 2nd and 4th sub-questions, which was about selling the data instead of storing it. A Wilcoxon signed rank test was used to examine whether knowledge, on what happens to their data, contributed to the feeling of violation of their privacy. Results

indicate a significant result between the 1st sub-question ($Mdn = 4.00$) and 3rd sub-question ($Mdn = 5.00$), with $V = 271, p < .001$. The same was done for the 2nd ($Mdn = 4.00$) and 4th ($Mdn = 5.00$) sub-question, again resulting in a significant result ($V = 202.5, p < .001$).

Chi-square tests were used to examine any difference between men and women in the sub-questions of question 9. All sub-questions were examined, but results indicate no significant result ($p > .05$ for all sub-questions).

The differences between higher educated people (HBO and above) and lower educated people were also examined with chi-square tests. Results indicate that there is a slight difference in the last sub-question of question 9, namely the violation of privacy when Facebook sells data without the user's knowledge. Higher educated people indicate they attach more value to this than lower educated people (i.e. higher educated people had relatively more "totally agree"), $\chi^2(5, N = 123) = 11.91, p = .036$. This is the opposite of what Zukowski & Brown (2007) found.

3.1.3 Usability & Data Sharing

For clarification purposes, the data categories and roles (explained in subsection 2.1) will be marked in the following paragraph as **bold** and *italic*, respectively.

As can be seen in Table 2, *researcher* has the lowest amount of "no" answer across all data categories, while *colleague* consistently has the highest amount of "no" answers. It is noticeable that the most individually shared category is **absence** for both *HR* and *manager*, and **sleep** is shared the least (i.e. the most "no" answers). For *colleague* this is **fitness** and **sleep**, respectively. The opposite can be seen for *researcher*, where **sleep** is the most individually shared, and **absence** is shared the least.

The data from Table 2 was used to make the privacy presets for people who do not wish to adjust every privacy setting manually. The result of this can be found in Table 3.

One third of the respondents (41 out of 123) indicate that they have become more aware of their privacy due to the questionnaire, while over 50% indicate that this is not the case. Some respondents noted that, while they have become more aware about their privacy for now, they will likely soon forget about it again.

3.2 Analytics

In total 51 unique visitors[10] visited the website in May, while there were only 18 participants in the trial. A unique visitor can not be traced back to a unique participant. These 51 unique visitors may include testers before and after the trial, as it is not possible to specify an exact date range to extract the data from. This could explain the amount of unique visitors in contrast to the amount of participants.

During the two-week trial, there was a total of 144 logged events (i.e. value changes) regarding the slider and a total of 22 events regarding the advanced privacy settings.

The 144 changes made with the slider were done so by nine unique visitors. This suggests that at most 9 out of the 18 participants (50%) changed their privacy settings with the slider. This takes into account that it is possible that multiple unique visitors can correspond to one participant. Nearly half of all the slider changes (65 out of 144) were made by 2 unique visitors.

It is possible to see in the log files that out of the 22 advanced privacy settings changes, 16 of these changes were canceling each other out, i.e., switches turned off and on again in quick succession by the same unique visitor. The other six changes were made by three unique visitors in total.

3.3 Follow-up Questionnaire

3.3.1 Quantitative

Out of the 18 trial participants, seven filled out the follow-up questionnaire, resulting in an overall response rate of 39%. These seven will now be referred to as "respondents". All respondents

[10] See subsubsection 2.4.1 for more information on unique visitors.

Table 2: Respondents' answers to sharing data with specific roles. The questions had the form of "Would you share **data category** with *role*?". More than half of the respondents indicated that they would share their individual data with researchers. Around 50% of the respondents indicated they will not share their data with their colleagues.

		Yes, individually	Yes, team level	No	Don't know
Sleep	Manager	15% *(19)*	21% *(26)*	59% *(72)*	5% *(6)*
	Colleague	20% *(25)*	20% *(24)*	52% *(64)*	8% *(10)*
	HR	26% *(32)*	22% *(27)*	48% *(59)*	4% *(5)*
	Researcher	63% *(77)*	20% *(25)*	8% *(10)*	8% *(10)*
Fitness	Manager	15% *(19)*	34% *(42)*	46% *(57)*	4% *(5)*
	Colleague	24% *(30)*	21% *(26)*	48% *(59)*	7% *(8)*
	HR	26% *(32)*	28% *(34)*	44% *(54)*	2% *(3)*
	Researcher	61% *(75)*	21% *(26)*	11% *(13)*	7% *(9)*
Absence	Manager	32% *(39)*	29% *(36)*	36% *(44)*	3% *(4)*
	Colleague	17% *(21)*	25% *(31)*	48% *(59)*	10% *(12)*
	HR	31% *(38)*	36% *(44)*	30% *(37)*	3% *(4)*
	Researcher	58% *(71)*	19% *(23)*	14% *(17)*	10% *(12)*
Stress	Manager	21% *(26)*	40% *(49)*	35% *(43)*	4% *(5)*
	Colleague	24% *(29)*	25% *(31)*	45% *(55)*	7% *(8)*
	HR	28% *(34)*	38% *(47)*	32% *(39)*	2% *(3)*
	Researcher	61% *(75)*	24% *(29)*	7% *(8)*	9% *(11)*
Performance	Manager	28% *(35)*	36% *(44)*	31% *(38)*	3% *(4)*
	Colleague	20% *(25)*	28% *(34)*	44% *(54)*	8% *(10)*
	HR	25% *(31)*	34% *(42)*	36% *(44)*	5% *(6)*
	Researcher	58% *(71)*	21% *(26)*	13% *(16)*	8% *(10)*
Motivation	Manager	20% *(24)*	40% *(49)*	38% *(47)*	2% *(3)*
	Colleague	21% *(26)*	26% *(32)*	45% *(55)*	8% *(10)*
	HR	23% *(28)*	37% *(46)*	36% *(44)*	4% *(5)*
	Researcher	56% *(69)*	24% *(29)*	11% *(13)*	10% *(12)*

Values in parentheses are number of respondents

indicated to have looked at their privacy settings; four of whom before the reminder was sent to all trial participants, and three after the reminder. The respondents who filled in their privacy settings after the reminder, all say that they did not know that they were able to adjust their privacy settings before they got the email.

The results of the SUS questionnaire can be seen in Table 4. The SUS score is calculated by adding the average of every question and multiplying it by 2.5. Using this scoring calculation, the overall score of the privacy settings is 73 out of 100, which is above the standard of 70 and can therefore be qualified as 'Good'.

3.3.2 Qualitative

Three out of the seven respondents indicated they missed something in the privacy settings. The most notable of which is one respondent who says that (s)he wished that (s)he could set the privacy settings manually, instead of using presets. This would suggest that the redirect link to the "advanced privacy settings", where you can set all settings manually, is not optimally displayed. The other 2 respondents indicated they missed a notification about privacy settings at the start of the application, and missed the feedback about what happens when changing the

Table 3: Privacy presets based on the results of the data sharing questions in the questionnaire.

		Manager	Colleague	HR	Researcher
Preset 1	Sleep	Team	Team	Team	Individual
	Enthusiasm	Team	Team	Team	Individual
	Motivation	Team	Team	Team	Individual
	Fitness	Team	Team	Team	Individual
	Burnout	Team	Team	Team	Individual
	Stress	Individual	Team	Team	Individual
Preset 2	Sleep	Don't share	Don't share	Don't share	Individual
	Enthusiasm	Team	Team	Team	Team
	Motivation	Team	Team	Team	Team
	Fitness	Team	Team	Team	Individual
	Burnout	Team	Team	Team	Individual
	Stress	Team	Team	Team	Individual
Preset 3	Sleep	Don't share	Don't share	Don't share	Individual
	Enthusiasm	Team	Team	Team	Team
	Motivation	Team	Team	Team	Team
	Fitness	Don't share	Don't share	Don't share	Individual
	Burnout	Team	Don't share	Team	Team
	Stress	Team	Don't share	Team	Individual
Preset 4	Sleep	Don't share	Don't share	Don't share	Individual
	Enthusiasm	Team	Team	Team	Team
	Motivation	Don't share	Don't share	Team	Team
	Fitness	Don't share	Don't share	Don't share	Team
	Burnout	Team	Don't share	Team	Team
	Stress	Don't share	Don't share	Team	Team
Preset 5	Sleep	Don't share	Don't share	Don't share	Team
	Enthusiasm	Don't share	Don't share	Don't share	Team
	Motivation	Don't share	Don't share	Don't share	Don't share
	Fitness	Don't share	Don't share	Don't share	Don't share
	Burnout	Team	Don't share	Team	Team
	Stress	Don't share	Don't share	Don't share	Team
Preset 6	Sleep	Don't share	Don't share	Don't share	Don't share
	Enthusiasm	Don't share	Don't share	Don't share	Don't share
	Motivation	Don't share	Don't share	Don't share	Don't share
	Fitness	Don't share	Don't share	Don't share	Don't share
	Burnout	Don't share	Don't share	Don't share	Don't share
	Stress	Don't share	Don't share	Don't share	Don't share

Table 4: Descriptive statistics of the SUS questionnaire regarding the privacy settings.

Questions		Minimum	Maximum	Average	SD
1.	I think that I would like to use the privacy settings frequently	0	4	.8	.84
2.	I found the privacy settings unnecessarily complex	4	0	3.6	.55
3.	I thought the privacy settings were easy to use	0	4	3.2	.84
4.	I think that I would need the support of a technical person to be able to use the privacy settings	4	0	4	0
5.	I found the various functions in the privacy settings were well integrated	0	4	2.4	.89
6.	I thought there was too much inconsistency in the privacy settings	4	0	3	.71
7.	I imagine that most people would learn to use the privacy settings very quickly	0	4	2.8	.84
8.	I found the privacy settings very awkward to use	4	0	3.2	.45
9.	I felt very confident using the privacy settings	0	4	2.8	.45
10.	I needed to learn a lot before I could get going with the privacy settings	4	0	3.4	.89

slider, respectively.

The last question in the questionnaire was optional feedback on the privacy settings, which 5 out of 7 respondents used. Most of the comments were positive remarks about the privacy settings. Something that came up was the fact that the description in the privacy settings screen may have been too long, and that some of the available privacy options were not yet incorporated into the dashboard itself. It was also suggested to make the privacy information available in more parts of the application. Another respondent said that it would be more logical to flip the slider scale around, meaning that the left side stands for very private (preset 6 in Table 3) and the right side for very open (preset 1 in Table 3). Furthermore, a respondent suggested that the default would be set at most private, or to make the current privacy settings explicit to the user. The default value was currently set at the least private preset (preset 1).

4 Discussion

The goal of this study was to provide insight into the usability of privacy settings in privacy dashboards. This was split up into two questions: how to inform the user intuitively about private data being shared; how to design the dashboard in a way that the user can exercise control on that data. The first question was answered by means of a questionnaire. The results of the questionnaire were used in the design and implementation of the privacy settings. The second question was answered by measuring the implemented design via web analytics and an extra questionnaire. Results indicate that the currently implemented privacy settings in the dashboard are acceptable as user-friendly, but the sample size was not large enough for any firm conclusions to be drawn.

4.1 Questionnaire

The age and education groups are very disproportionate to a real world scenario. On January 1 2016, about 12% of the Dutch population was between 20 and 29 years old, and nearly 23% was

highly educated (HBO or above). (Centraal Bureau voor de Statistiek, 2016a). In this study those groups are 54% and 80%, respectively. Some other groups are under-represented, such as 0–19, who are very active online (Centraal Bureau voor de Statistiek, 2016c). It is possible that these groups are disproportionate due to the fact that the questionnaire was distributed over social media. It is not clear how this may have affected the results.

Zukowski & Brown (2007) found that younger internet users are less concerned about their privacy; and internet users with higher education are also less concerned about their privacy. However, on one question (question 9.4), higher educated people indicate that they feel that their privacy is violated more so than lower educated people. This is the opposite of what Zukowski & Brown (2007) found. A contributing factor to this finding might be the underrepresentation of the lower educated people ($n = 25$) in contrast to overrepresentation of higher educated people ($n = 98$). It is also hard to tell the difference in privacy concerns on the basis of one sub-question. The other (sub-)questions give p-values that are less than significant ($p > .05$).

The fact that no significant difference was found between men and women is supported by Zukowski & Brown (2007).

Results have shown that "absence" was the most individually shared data category for both manager and HR roles. This could be explained by the fact that both roles (should) already have this information, and is therefore considered not a violation of privacy. Sleep is least shared individually—except with researchers—which could be argued was one of the more private categories in the questionnaire, and is therefore shared the least.

Finally, results have shown that one third of the respondents have become more aware of their privacy, but comments showed that some will likely not act on their intentions to remedy their shortcomings on this subject. According to Sheeran (2002), there is a gap between the intention of doing something and actually doing it, namely the intention-behavior gap. This could also be the case for privacy settings, as most people indicate they find it important, but do not act on the matter.

4.2 Analytics

Results indicated that many of the logged slider events, were logged in quick succession, sometimes with only seconds in between. It is possible that the users understood the purpose of the slider perfectly, and changed the settings very quickly. It is also possible that people could not make up their mind and dragged the slider back and forth. However, it can also suggest that it was not entirely clear what the slider did. A problem with the slider was the changing text. To read all the descriptions for the presets, at least 5 slider changes were necessary. Imagine a scenario where a user reads all 6 presets, but wants to go back to the first option. Not only does this lead to many logged events—10 to be exact—but it also requires more actions from the user, which is not user-friendly.

Results have shown that only a small amount of participants used the advanced privacy settings, and thus there is not enough data to draw any conclusion. An explanation can be that the advanced privacy settings were not found at all. A solution for this could be to make the advanced privacy settings stand out more in the text, to draw attention of the user. Another solution could be to force users to look at the privacy settings, because they might have the intention to change the privacy settings, but do not act on this due to the intention-behavior gap (Sheeran, 2002).

The first questionnaire showed that people indicated that it was important to both control and understand their data, but the field test indicated that only half of all the participants changed their privacy settings. An explanation can be that people did not find the privacy settings at all (more on that in subsection 4.3), another explanation can be, as mentioned above, the difference between intention and actual behavior (Sheeran, 2002). It is also possible that participants in the trial trusted TNO with their data, as the participants were TNO employees, and trusted that nothing would happen to their data. This is supported by Lederer et al. (2003), who says that the "who" is very important in trust. This could have an impact on the results, as they would not feel the need to use the privacy settings as much.

Web analytics is a relative new form of evaluating websites in comparison with other methods (e.g. surveys), as Piwik itself has only existed for approximately 10 years. This can lead to some problems, because not all features have been explored in research yet. Many questionnaires used in research are validated, but web analytics is much harder to validate due to its many capabilities. Based on the experience of this research, the data and results of the web analytics look promising. This indicates that web analytics can certainly be used for future research. I would advice to look at the many possible features that are available by web analytic platforms, such as Piwik. This thesis only used custom made events, while a large array of tools is offered by analytics platforms. And while the custom events are very useful, it is not nearly the full potential of web analytics. Analytics platforms are a very powerful tools for analyzing websites, but if the data is not understood properly, it is a very hard tool to use (Phippen et al., 2004).

4.3 Follow-up Questionnaire

Results seem to indicate that the current implementation of the design is acceptable. The score of 73 is marked by Bangor et al. (2009) as "Good", and by their standards an acceptable score. This result is also above the goal, which was set in subsection 2.7. However, due to a temporary error in the questionnaire, 2 out of 7 respondents did not fill out the translated SUS, resulting in 5 completed SUS questionnaires. Unfortunately, with $n = 5$, the results of the SUS only give an indication of the usability of the privacy settings, but can not be used to draw any conclusions.

Furthermore, while the original SUS is widely used, the (self) translated Dutch version is not, and thus it is possible that there were some ambiguous questions. The translated version was checked by multiple peers, to minimize the ambiguity. The impact of this on the findings is unknown.

Results show that some people did not know that they were able to adjust their privacy settings at all. This would suggest that the privacy settings option is not yet optimally displayed. However, the privacy settings button was situated next to the "home" button, which was used, at least once, by 21 unique visitors (in contrast to the 9 that used the privacy settings). An explanation could be that the participants did not look at all the options in the menu, or the privacy settings did not stand out enough.

The results of the additional feedback, at the end of the questionnaire, suggest an opt-in scenario than the currently implemented opt-out. Madrian & Shea (2001) found that automatic enrollment (opt-out) dramatically increases the participation rate, which suggests that people tend to stay at the default setting. Respondents also suggest to show what happens to their data on the specific subject, i.e. show what happens to their sleep data when they access that specific page. This is in line with the results that insight into data is more important than control.

4.4 Conclusion

The first research question was “How can users be informed intuitively about the use of their personal data in a privacy dashboard?”. Results have shown that people are significantly more concerned about who they share their data with, than if they can control their data (this does not mean, however, that control is not also important).

The second research question was “How can a privacy dashboard be designed in a way that it helps the user understand what happens to his data and how the user can control this?”. Some people do not wish to set all the privacy settings manually, as this is neither user-friendly, nor convenient for less-technical people. In this thesis, the solution for these people was to implement a slider with privacy presets.

The results from the web analysis are all but conclusive. The privacy settings were not used enough to draw any meaningful conclusions to indicate that the privacy settings were designed and implemented in an intuitive way to help the user understand what happens to his data or how to control it. Results indicated that a slider does not look like a practical tool for this problem, and is therefore discouraged for future use. However, the question about which method is user-friendly and convenient remains to be solved.

The results from the follow-up questionnaire showed that some people did not know that they could adjust the privacy settings. Furthermore, results carefully indicated that the privacy settings in its current design is acceptable as user-friendly. However, based on the very low amount of respondents on the follow-up questionnaire, it is not possible to draw any conclusion at this time.

4.5 Recommendations & Future Work

Insight into personal data is very important for users, it is therefore recommended to have an overall privacy settings feature built into the dashboard to inform the users about the use of their private information.

Furthermore, it is recommended to show users what happens to their data on the relevant screens, i.e., show what happens to sleep data when the user is on the screen involving sleep data.

The privacy settings should be designed so that it is in one place, which is easy to find. Results indicate that this was not the case in the current implementation, where it was located in the menu. A solution for this problem could be to give an explicit, yet non-intrusive, reminder about the privacy settings, when starting the application the first time. This solution might provide an increase in usability factors such as *Ease of Navigation*, and *Ease of Learning*, which in turn could increase the trust of the application (Roy et al., 2001). Another solution might be to make the privacy settings stand out more by using different icons or larger fonts, for example. As the analytics results have shown, there were hardly any participants on the advanced privacy settings page. This is also a problem that might arise from the fact that it does not stand out enough. An explanation for this might be that the link to the advanced privacy settings is not explicit enough about its destination, i.e. the text is not explanatory enough. A solution for this might be to change the text, or to use another method to link to the advanced privacy settings. While the main rule is to use links instead of buttons for navigation purposes (Nielsen, 2007), another method may be better in this case. More research could be done on the potential solutions mentioned above.

The slider was implemented for its perception and ease of learning, as the slider stands out of text and is very straightforward to use. However, based on the analytics results and the additional feedback of the follow-up questionnaire, it shows that the slider was, in fact, not very intuitive in controlling the privacy settings. Using the slider made it very clear that something was happening to the privacy settings, but it was not clear what that was exactly. The recommendation of this thesis is to find different method to change privacy settings, without forcing the user to manually set everything by himself, as this would diminish ease of learning. Which method should take the sliders' place, can be explored in future research.

Finally, the impact of the opt-in or opt-out approach of the privacy settings is unknown. Whether an opt-in or opt-out approach should be used for privacy settings is a topic for future research.

References

3Doc. (2016). *Addicted To My Phone.* Retrieved from http://www.uitzendinggemist.net/aflevering/366703/3doc.html

Bangor, A., Kortum, P., & Miller, J. (2009). Determining what individual SUS scores mean: Adding an adjective rating scale. *Journal of usability studies*, *4*(3), 114–123. Retrieved from http://66.39.39.113/upa_publications/jus/2009may/JUS_Bangor_May2009.pdf doi: 66.39.39.113

Bedi, P., & Banati, H. (2006). *Assessing User Trust to Improve Web Usability* (Vol. 2) (No. 3). doi: 10.3844/jcssp.2006.283.287

Brooke, J. (1996). SUS - A quick and dirty usability scale. *Usability evaluation in industry*, *189*(194), 4–7. Retrieved from http://hci.liacs.nl/files/SUS-questionaire.pdf

Centraal Bureau voor de Statistiek. (2016a). *Bevolking; geslacht, leeftijd en burgerlijke staat, 1 januari.* Retrieved from http://statline.cbs.nl/Statweb/publication/?DM=SLNL&PA=7461BEV&D1=0&D2=a&D3=0,123-126,131,l&D4=l&HDR=T,G3,G1&STB=G2&VW=T

Centraal Bureau voor de Statistiek. (2016b). *Bevolking; hoogst behaald onderwijsniveau; geslacht, leeftijd en herkomst.* Retrieved from http://statline.cbs.nl/Statweb/publication/?DM=SLNL&PA=82275NED&D1=0&D2=0&D3=0&D4=0&D5=0,2-4,8-10,12-14&D6=69&HDR=T,G1,G3,G5&STB=G2,G4&VW=T

Centraal Bureau voor de Statistiek. (2016c). *Internet; toegang, gebruik en faciliteiten.* Retrieved from http://statline.cbs.nl/Statweb/publication/?DM=SLNL&PA=83429NED&D1=0,2-5&D2=0,3-7,15-19&D3=0&D4=a&HDR=T&STB=G1,G2,G3&VW=T

Cheskin Research, & Studio Archetype/Sapient. (1999). *eCommerce Trust Study.* Retrieved from http://web.archive.org/web/20000115125857/http://www.studioarchetype.com/cheskin/

de Vos, H., Claas, L., Spek, J., de Boer, J., Van, M., & Barca, C. C. (2016). *PIME WP2 Technology Experimentation End report* (Tech. Rep. No. December).

EU Directive. (1995). 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. *Official Journal of the EC*, *23*(6). Retrieved from http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:EN:HTML

Few, S. (2004). Dashboard Confusion. *Intelligent Enterprise*.

Few, S. (2006). *Information Dashboard Design: The Effective Visual Communication of Data.* O'Reilly Media, Inc.

Fogg, B. J., Tseng, H., Hall, C., & Drive, H. (1999). Elements of computer credibility. *Conference on Human Factors in Computing Systems - Proceedings*(May), 80–87. doi: 10.1145/302979.303001

Grande, D., Asch, D. A., Wan, F., Bradbury, A. R., Jagsi, R., & Mitra, N. (2015). Are Patients With Cancer Less Willing to Share Their Health Information? Privacy, Sensitivity, and Social Purpose. *Journal of Oncology Practice*, *11*(5), 378–383. Retrieved from http://jop.ascopubs.org/content/11/5/378.abstract doi: 10.1200/JOP.2015.004820

Hoepman, J.-H. (2014). Privacy design strategies. In *Ifip international information security conference* (pp. 446–459). Retrieved from http://arxiv.org/abs/1210.6621 doi: 10.1007/978-3-642-55415-5

IDC. (2016). *Smartphone Market Share.* Retrieved from http://www.idc.com/promo/smartphone-market-share/os

Jacobsen, I., Booch, G., & Rumbaugh, J. (1999). *The unified software development process.* Addison-wesley Reading.

Jøsang, A., Keser, C., & Dimitrakos, T. (2005). Can We Manage Trust? *Trust Management*, *3477*(May 2005), 93–107. Retrieved from https://link.springer.com/chapter/10.1007%2F11429760_7 doi: http://dx.doi.org/10.1007/11429760{_}7

Kim, J., & Moon, J. Y. (1998). Designing towards emotional usability in customer interfaces—trustworthiness of cyber-banking system interfaces. *Interacting with Computers*, *10*(97), 1–29. doi: 10.1016/S0953-5438(97)00037-4

Lederer, S., Mankoff, J., & Dey, A. K. (2003). Who wants to know what when? privacy preference determinants in ubiquitous computing. *CHI '03 extended abstracts on Human factors in computing systems - CHI '03*, 724. Retrieved from http://portal.acm.org/citation.cfm?doid=765891.765952 doi: 10.1145/765891.765952

Madrian, B. C., & Shea, D. F. (2001). The Power of Suggestion: Inertia in 401(k) Participation and Savings Behavior. *The Quarterly Journal of Economics*, *CXVI*(November). Retrieved from http://www.retirementmadesimpler.org/Library/ThePowerofSuggestion-Inertiain401(k).pdf

Nielsen. (2007). *Command Links.* Retrieved from https://www.nngroup.com/articles/command-links/

Nielsen, J., & Norman, D. A. (2000). *Usability On The Web Isn't A Luxury.* Retrieved from https://web.archive.org/web/20070104174722/http://www.informationweek.com/773/web.htm

Phelps, J., Nowak, G., & Ferrell, E. (2000). Privacy Concerns and Consumer Willingness to Provide Personal Information. *Journal of Public Policy & Marketing*, *19*(1), 27–41. doi: 10.1509/jppm.19.1.27.16941

Phippen, A., Sheppard, L., & Furnell, S. (2004). A practical evaluation of Web analytics. *Internet Research*, *14*(4), 284–293. Retrieved from http://www.emeraldinsight.com/doi/10.1108/10662240410555306 doi: 10.1108/10662240410555306

Roy, M. C., Dewit, O., & Aubert, B. A. (2001). The impact of interface usability on trust in web retailers. *Internet research*, *11*(5), 388–398. doi: 10.1108/10662240110410165

Sankar, P., Moran, S., Merz, J. F., & Jones, N. L. (2003). Patient perspectives on medical confidentiality. *Journal of General Internal Medicine*, *18*(8), 659–669. doi: 10.1046/j.1525-1497.2003.20823.x

Sasse, M. (2005). Usability and Trust in Information Systems. *Cyber Trust Crime Prevention Project University College London*, 1–18. Retrieved from http://discovery.ucl.ac.uk/20346/

Sheeran, P. (2002). Intention-Behavior Relations: A Conceptual and Empirical Review. *European Review of Social Psychology*, *12*(1), 1–36. doi: 10.1080/14792772143000003

Statista. (2016). *Apps available in play store.* Retrieved from https://www.statista.com/statistics/266210/number-of-available-applications-in-the-google-play-store/

Truven Health Analytics. (2015). *Data Privacy , Part 2 Executive Summary* (No. January).

Westin, A. F. (2003). Social and political dimensions of privacy. *Journal of social issues*, *59*(2), 431–453.

Yoon, S. J. (2002). The antecedents and consequences of trust in online-purchase decisions. *Journal of Interactive Marketing*, *16*(2), 47–63. doi: 10.1002/dir.10008

Zimmermann, C., Accorsi, R., & Müller, G. (2014). Privacy dashboards: reconciling data-driven business models and privacy. In *Availability, reliability and security (ares), 2014 ninth international conference on* (pp. 152–157).

Zukowski, T., & Brown, I. (2007). Examining the Influence of Demographic Factors on Internet Users' Information Privacy Concerns. *Saicsit 2007*(October), 197–204. doi: 10.1145/1292491.1292514

A Questionnaire

Questionnaire Privacy & Usability

Introductie

Hartelijk dank voor het deelnemen aan dit onderzoek. Deze vragenlijst gaat voornamelijk over privacy en usability. Het doel van de vragenlijst is om de wensen en verwachtingen van de gebruikers duidelijk te krijgen. Bij de meeste vragen is het mogelijk om toelichting te geven bij uw antwoord. Hoewel dit niet verplicht is, kan het zeker helpen bij het verwerken van de data voor de bovengenoemde doeleinden. Verplichte vragen zullen worden aangegeven met een *.

Deelname aan dit onderzoek is anoniem. Er zullen geen identificerende persoonsgegevens worden verwerkt.

De vragenlijst zal ongeveer 10 minuten in beslag nemen.

Voor eventuele vragen over dit onderzoek kunt u contact opnemen met stef.vangogh@tno.nl

Questionnaire Privacy & Usability

Demografische vragen

* 1. In welke leeftijdsgroep zit u?

- ◯ 0-19
- ◯ 20-29
- ◯ 30-39
- ◯ 40-49
- ◯ 50-59
- ◯ 60+

* 2. Wat is uw geslacht?

- ◯ Man
- ◯ Vrouw

* 3. Wat is uw hoogst genoten opleiding?

- ◯ Basisonderwijs / lagere school
- ◯ LBO / VBO / VMBO
- ◯ Middelbaar beroepsonderwijs (MBO)
- ◯ Hoger voortgezet onderwijs (HAVO of VWO)
- ◯ Hoger beroepsonderwijs (HBO)
- ◯ Wetenschappelijk onderwijs (Universiteit)

* 4. Wat is het besturingssysteem van uw mobiele telefoon?

- ◯ Google Android
- ◯ Apple iOS
- ◯ Blackberry
- ◯ Windows Phone (Microsoft)
- ◯ Anders, namelijk:

Questionnaire Privacy & Usability

Privacy

De volgende vragen zullen gaan over privacy en het gevoel van privacy. Toelichtingen bij de vragen zijn niet verplicht, maar kunnen wel gebruikt worden om duidelijk te maken waarom u dat antwoord gekozen heeft.

* 5. In hoeverre is het belangrijk voor u om controle te hebben over het delen van uw data?

Zeer onbelangrijk	Onbelangrijk	Neutraal	Belangrijk	Zeer belangrijk
◯	◯	◯	◯	◯

6. Toelichting

* 7. In hoeverre is het belangrijk voor u om inzicht te hebben over met wie u uw data deelt?

Zeer onbelangrijk	Onbelangrijk	Neutraal	Belangrijk	Zeer belangrijk
◯	◯	◯	◯	◯

8. Toelichting

* 9. Geef aan in hoeverre u het met de stellingen eens bent.

Ik vind het een schending van mijn privacy als ...

	Helemaal mee oneens	Mee oneens	Neutraal	Mee eens	Helemaal mee eens	Weet ik niet
Facebook, met mijn medeweten, al mijn gegevens en foto's heeft opgeslagen op een plek waar ik geen invloed meer kan uitoefenen.	○	○	○	○	○	○
Facebook, met mijn medeweten, al mijn gegevens en foto's doorverkoopt.	○	○	○	○	○	○
Facebook, zonder mijn medeweten, al mijn gegevens en foto's heeft opgeslagen op een plek waar ik geen invloed meer kan uitoefenen.	○	○	○	○	○	○
Facebook, zonder mijn medeweten, al mijn gegevens en foto's doorverkoopt.	○	○	○	○	○	○

10. Toelichting

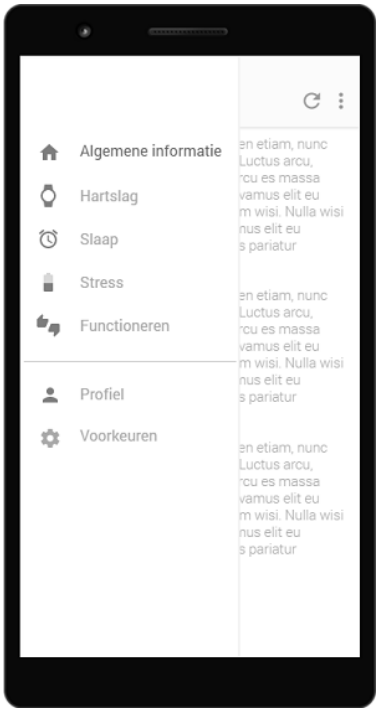
* 11. Geef aan voor de volgende stelling in hoeverre u het hier mee eens bent.

	Helemaal mee oneens	Mee oneens	Neutraal	Mee eens	Helemaal mee eens
Ik vind het een probleem als een app, zonder mijn toestemming, mijn locatie kan opslaan.	○	○	○	○	○
Ik vind het een probleem als een app, zonder mijn toestemming, mijn microfoon kan aanzetten.	○	○	○	○	○
Ik vind het een probleem als een app, zonder mijn toestemming, mijn gesprekken kan opnemen.	○	○	○	○	○

Questionnaire Privacy & Usability

Usability

De volgende vragen zullen gaan over gebruiksvriendelijkheid.
Stel u voor dat u de onderstaande app gebruikt om persoonlijke gegevens bij te houden van een smartwatch, zoals de kwaliteit van uw slaap.



* 12. Zie de afbeelding bovenaan de pagina. Stel dat u wilt inzien met wie u uw data over stress deelt. Waar verwacht u dit te vinden? (Er zijn meerdere antwoorden mogelijk)

- [ ] Stress
- [ ] Profiel
- [ ] Voorkeuren
- [ ] Algemene informatie
- [ ] Hartslag
- [ ] Slaap
- [ ] Functioneren
- [ ] Anders, namelijk:

13. Toelichting

* 14. Zie de afbeelding bovenaan de pagina. Stel dat u wilt inzien met wie u uw data over stress deelt. Waar wenst u dit te vinden? (Er zijn meerdere antwoorden mogelijk)

- [ ] Stress
- [ ] Profiel
- [ ] Voorkeuren
- [ ] Algemene informatie
- [ ] Hartslag
- [ ] Slaap
- [ ] Functioneren
- [ ] Anders, namelijk:

15. Toelichting

* 16. U wilt instellen met wie u uw data deelt. Wilt u de privacy instellingen per data soort kunnen instellen (bv. hartslag, stress) of wilt u het voor alle data tegelijkertijd kunnen instellen?

- ◯ Per categorie
- ◯ Tegelijkertijd
- ◯ Weet ik niet

17. Toelichting

Questionnaire Privacy & Usability

Gegevens delen

De volgende vragen zullen gaan over het delen van bepaalde privacy gevoelige gegevens. Gegevens delen kan handig zijn voor het tijdig ingrijpen als eventuele hulp nodig is. Het kan ook handig zijn voor een leidinggevende om een team goed aan te sturen.

* 18. Zou je de volgende geanonimiseerde data met je leidinggevende delen?

	Nee	Ja, als teamgemiddelde	Ja, op individueel niveau	Weet ik niet
Stressniveau	◯	◯	◯	◯
Kwaliteit van slaap	◯	◯	◯	◯
Functioneren op werk	◯	◯	◯	◯
Fitheid	◯	◯	◯	◯
Motivatie	◯	◯	◯	◯
Verzuim	◯	◯	◯	◯

19. Toelichting

* 20. Zou je de volgende geanonimiseerde data met Human Resources delen?

	Nee	Ja, als teamgemiddelde	Ja, op individueel niveau	Weet ik niet
Stressniveau	○	○	○	○
Kwaliteit van slaap	○	○	○	○
Functioneren op werk	○	○	○	○
Fitheid	○	○	○	○
Motivatie	○	○	○	○
Verzuim	○	○	○	○

21. Toelichting

* 22. Zou je de volgende geanonimiseerde data met je collega delen?

	Nee	Ja, als teamgemiddelde	Ja, op individueel niveau	Weet ik niet
Stressniveau	○	○	○	○
Kwaliteit van slaap	○	○	○	○
Functioneren op werk	○	○	○	○
Fitheid	○	○	○	○
Motivatie	○	○	○	○
Verzuim	○	○	○	○

23. Toelichting

* 24. Zou je de volgende geanonimiseerde data met onderzoekers delen?

	Nee	Ja, als teamgemiddelde	Ja, op individueel niveau	Weet ik niet
Stressniveau	○	○	○	○
Kwaliteit van slaap	○	○	○	○
Functioneren op werk	○	○	○	○
Fitheid	○	○	○	○
Motivatie	○	○	○	○
Verzuim	○	○	○	○

25. Toelichting

Questionnaire Privacy & Usability

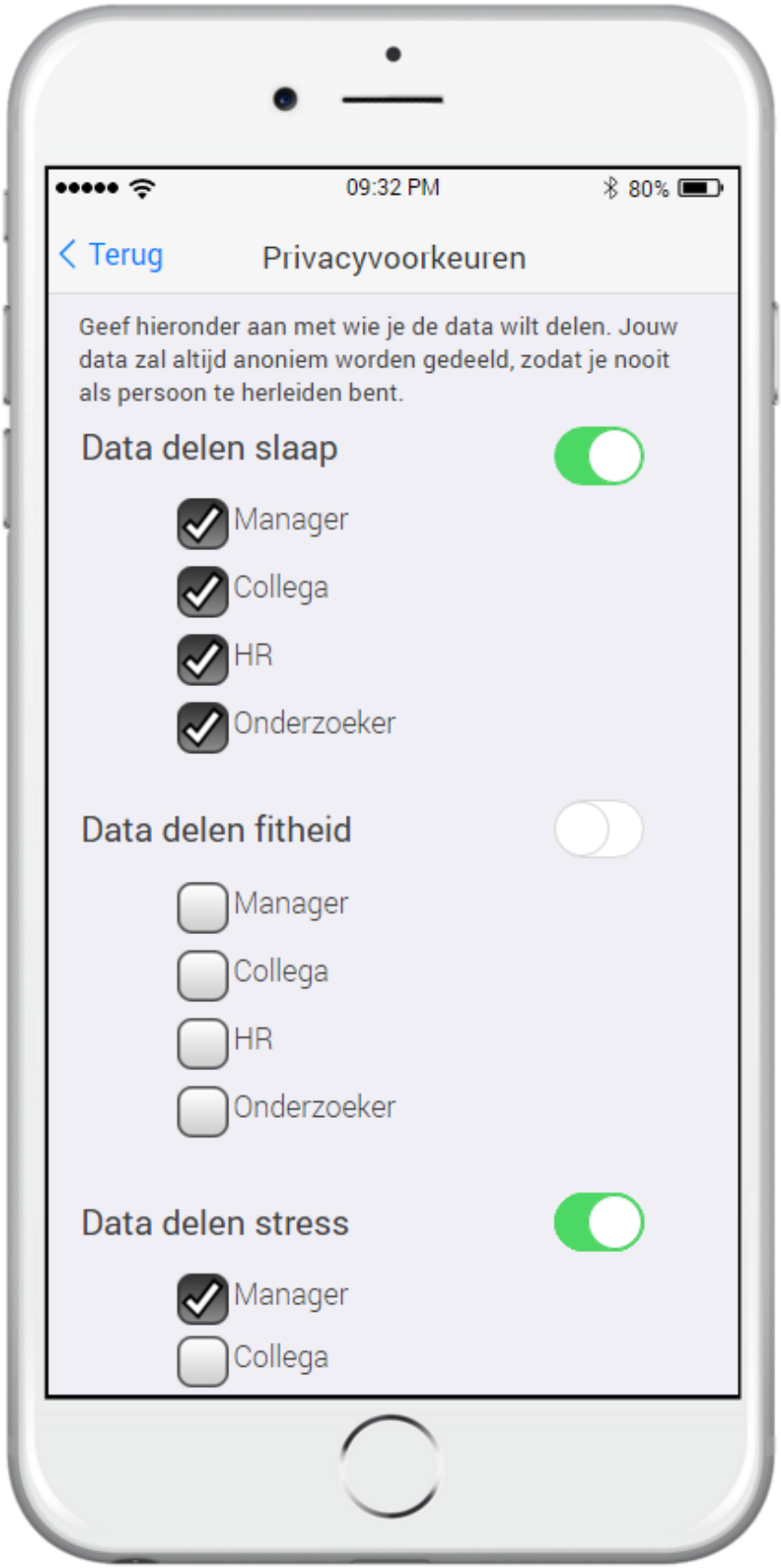
* 26. Bent u door deze vragenlijst meer bewust geworden van uw privacy?

- Ja
- Nee
- Weet ik niet

27. Toelichting

B Screen Design Privacy Settings

C Screen Design Advanced Privacy Settings



D Follow-up Questionnaire

Nameting Privacy Menselijke Veerkracht

Introductie

Hartelijk dank voor het deelnemen aan dit onderzoek. Deze vragenlijst gaat over de gebruiksvriendelijkheid van de privacyinstellingen in het dashboard 'Menselijke Veerkracht', waar u de afgelopen 2 weken mee gewerkt heeft. Het doel van de vragenlijst is om door middel van uw feedback de gebruiksvriendelijkheid van de privacyinstellingen te verbeteren. Aan het einde van de vragenlijst zal de mogelijkheid zijn tot extra feedback. Verplichte vragen zullen worden aangegeven met een *.

Deelname aan dit onderzoek is anoniem. Er zullen geen identificerende persoonsgegevens worden verwerkt.

De vragenlijst zal een paar minuten in beslag nemen.

Voor eventuele vragen over dit onderzoek kunt u contact opnemen met stef.vangogh@tno.nl

Nameting Privacy Menselijke Veerkracht

Privacyinstellingen

1. Heeft u uw privacyinstellingen aangepast in het Menselijke Veerkracht dashboard?

- ◯ Ja
- ◯ Nee

Nameting Privacy Menselijke Veerkracht

Privacyinstellingen

2. Heeft u uw privacyinstellingen aangepast vóór of ná de herrineringsmail?

- ◯ Voor
- ◯ Na

Nameting Privacy Menselijke Veerkracht

Privacyinstellingen

* 3. Waarom heeft u de instellingen ná de herrineringsmail ingevuld?

- ☐ Ik ben het vergeten
- ☐ Ik wist niet dat ik mijn privacy instellingen kon aanpassen
- ☐ Anders, namelijk:

Nameting Privacy Menselijke Veerkracht

Privacyinstellingen

4. Waarom heeft u uw privacyinstellingen niet aangepast?

- [ ] Ik heb de optie niet gevonden
- [ ] Ik heb de behoefte niet om mijn privacy instellingen aan te passen
- [ ] Ik ben het vergeten
- [ ] Anders, namelijk:

Nameting Privacy Menselijke Veerkracht

Gebruiksvriendelijkheid Privacyinstellingen

De volgende stellingen gaan over het gebruik en gebruikersvriendelijkheid van de privacyinstellingen.

* 5. Ik denk dat ik de privacyinstellingen vaak zou willen gebruiken

Helemaal niet mee eens				Helemaal mee eens
○	○	○	○	○

* 6. Ik vond de privacyinstellingen onnodig moeilijk

Helemaal niet mee eens				Helemaal mee eens
○	○	○	○	○

* 7. Ik vond het makkelijk om de privacyinstellingen te gebruiken

Helemaal niet mee eens				Helemaal mee eens
○	○	○	○	○

* 8. Ik denk dat ik hulp van een technisch persoon nodig heb om de privacyinstellingen te kunnen gebruiken

Helemaal niet mee eens				Helemaal mee eens
○	○	○	○	○

* 9. Ik vond dat de privacyinstellingen goed in het dashboard waren geïntegreerd

Helemaal niet mee eens				Helemaal mee eens
○	○	○	○	○

* 10. Ik vond dat er te veel inconsistenties waren in de privacyinstellingen

Helemaal niet mee eens				Helemaal mee eens
○	○	○	○	○

* 11. Ik kan me voorstellen dat de meeste mensen de privacyinstellingen snel onder de knie zullen krijgen

Helemaal niet mee eens				Helemaal mee eens
○	○	○	○	○

* 12. Ik vond de privacyinstellingen erg onhandig

Helemaal niet mee eens				Helemaal mee eens
○	○	○	○	○

* 13. Tijdens het gebruik van de privacyinstellingen wist ik goed waar ik mee bezig was

Helemaal niet mee eens				Helemaal mee eens
○	○	○	○	○

* 14. Ik moest veel leren over het systeem voordat ik aan de slag kon met de privacyinstellingen

Helemaal niet mee eens				Helemaal mee eens
○	○	○	○	○

Nameting Privacy Menselijke Veerkracht

* 15. Ik miste iets bij de privacyinstellingen

- ○ Ja
- ○ Nee

Nameting Privacy Menselijke Veerkracht

* 16. Wat miste u bij de privacyinstellingen?

Nameting Privacy Menselijke Veerkracht

17. Heeft u nog op- of aanmerkingen over de privacyinstellingen?