D8.5

Pilot case evaluation report and lessons learned – v2

v 1.1 / 2016-10-27

Rob Heyman (iMinds), Ali Padyab (LTU), Laurence Claeys (iMinds), Jo Pierson (iMinds), Marita Holst (LTU), Abdolrasoul Habibipour (LTU)

Abstract
This deliverable presents the design and findings of the second round of pilots conducted within USEMP. It is a follow up from D8.3 ("Pilot case evaluation report and lessons learned - v1"). We aim at evaluating the DataBait tool on two levels. On the first level this evaluation consists of the changes implemented by technical partners and on the second level, we evaluate the extra information iMinds has added to inform users of implications and solutions.

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 8	
Deliverable lead org.	iMinds
Deliverable type	Report
Authors	Rob Heyman (iMinds), Ali Padyab (LTU), Laurence Claeys (iMinds), Jo Pierson (iMinds), Marita Holst (LTU)
Reviewers	Giorgos Petkos, Eleftherios Spyromitros-Xioufis, Andreas Drakos
Version	1.2
Status	Final
Dissemination level	PU: Public
Due date	2016-09-30
Delivery date	2016-09-30 (revised 2017-04-20 after reviewers' comments)

Table of Contents

1 Introduction

This deliverable presents the design and findings of the second round of pilots conducted within USEMP. It follows up D8.3 (“Pilot case evaluation report and lessons learned - v1”) that reported on the first round of pilots. We evaluate the changes and updates sparked by the results of D8.3, our technical partners’ progress and the changes we made with regard to the information provided on DataBait.

The deliverable is structured as follows: In the rest of this introductory section we first frame the objectives and then present the research outset. Subsequently, in section 2 we look into the pilot methodology and living lab tasks and then, on the final section we report on our findings.

1.1 Objectives and research questions

The objective of this deliverable is to report on the results of the pilot and where necessary provide suggestions on improvements of the platform. In order to do so, we evaluate features during the pilot similar to D8.3.

We designed the following research questions to evaluate DataBait as a tool to increase awareness with regard to users’ digital footprint:

1. Where should we further improve the ease of use of the different DataBait tools?
2. Is DataBait a Privacy Enhancing Technology (PET) that can increase user awareness with regard to information disclosed on social media and through cookies?
3. Does DataBait offer users actionable information to revise their online and social media disclosure?

Next to these general questions, technical partners have added new features to respond to issues identified in D8.3[1]. As such, we practice what we preach and implement an iterative living lab approach where end-users are able to impact design through participation in the pilots. An overview of all issues identified during the first round of pilots and their status can be found in Table 1.

[1]In some cases, the suggested changes were not implemented in the pilot direclty, but in the survey. We therefore labeled the status of these as ‘Implemented in pilot survey'. This allows us to test the given solution without spending development effort on features that still require extensive evaluation.

Component	Problem	Solution	status
Registration	Lack of a confirmation message	Add a confirmation message	Implemented
	In some cases a loading animation kept users waiting while the service was down.	The status of the server should be communicated to the DataBait client.	It wasn't possible to implement the solution in the pilot.
DLA	DLA text is too long and technical	Add a summary of the DLA	We test this in the current pilot
Trackers	Not clear what trackers can do with this information	Add more information	Implemented
	Blocking only applied to a particular tracker on particular website	Have a general block function	Not added
	Users have no idea what trackers do	Add more information	Implemented
	Unzipping the plugin was difficult	Add it without file compression	Implemented
Audience influence statistical data	Does not show any information if no friends are on DataBait	Explanatory text added: functionality limited by FB API restrictions	Implemented
Audience influence, detailed interactions	Detailed interactions are moving around	Detailed interactions should not move	Could not be changed
	Dead links behind detailed interactions are annoying	Make sure all links work	Implemented
	Old interactions are not that relevant and are perceived as clutter	Have a way to prioritize more recent news	Will be added after the current pilot
Image leaks	Users had to wait quite long for this feature	Add a warning for long loading times more prominently	Implemented
	Concepts only partly fit the frame	Make these concepts fit the screen	Implemented
	Firefox plugin blocked loading of the website	Make sure this does not happen	Implemented
General	Users do not read additional information	Find new ways to increase use of additional information	Implemented

Table 1: Overview of issues identified during the first round of pilots and solutions

Lastly, compared to the first round of pilots, one component was changed and another was added:

- Image leaks existed in the previous of version of the tool that was tested during the first round of pilots. In order to make better use of Image leaks, users are now able to see green or red borders around pictures that alert them about possibly sensitive content. This effectively prompts the users to reconsider the sharing of images that are flagged as sensitive by DataBait. Secondly, users are now able to provide feedback in order to improve the accuracy of the sensitive content detection algorithm.This feedback is eventually used to improve the accuracy of the sensitive content detection algorithm. For more details please see D5.6.
- Your disclosure scoring. This is a new component that includes two sub-components. The first is the disclosure scoring framework that provides to the users an overview of their disclosed information organized in a number of 'dimensions' (e.g. the 'demographics' dimension includes information about the users' gender, age, nationality, etc.). For each type of information or dimension, a number of scores that quantify different aspects of information disclosure are provided to the user, the most important of which is the overall disclosure score. Importantly, the scoring framework comes with a number of inference modules that analyze the OSN data of users and feed their results into the scoring framework. The second sub-component is a control assistance tool that lists particular pieces of content that have a high contribution to the user's overall disclosure score and which the user may like to reconsider sharing. For more details please see D6.5.

1.2 Living lab outset

In this part we shortly summarize our living lab outset by situating this deliverable within the previous deliverables. The first pilot consisted of the version of DataBait that went live on January 15, 2016. This pilot takes into account the changes we have implemented based on the results of the first deliverable .

We already referred to the different accents in the two pilots reported in D8.3 and here. The first pilot is small scale and exploratory to answer the following research question: “What should be added to DataBait to offer users actionable information with regard to their social media and online information disclosure?”. The first pilot emphasized this question more, but it also looked into the other research questions, that is, it also looked into usability and increase of awareness as researched in D8.2, but with a living lab method.

In this pilot, we evaluate the newly found means to render awareness meaningful to change personal data flows together with the evaluation of other changes to ease of use and increasing awareness of users.

2 Method: Living lab

The main aim of the second living lab pilot is to test the changes that have been integrated in DataBait by the end of May. Secondly, we want to gather feedback with regard to the extra information we provide about the use of DataBait. This means asking the users through open questions how they felt about the information we provided them and how they wished to proceed further with that information. Next we we will suggest to our partners to find solutions for the problems respondents made us aware of.

This living lab approach is structured as shown in Figure 1.

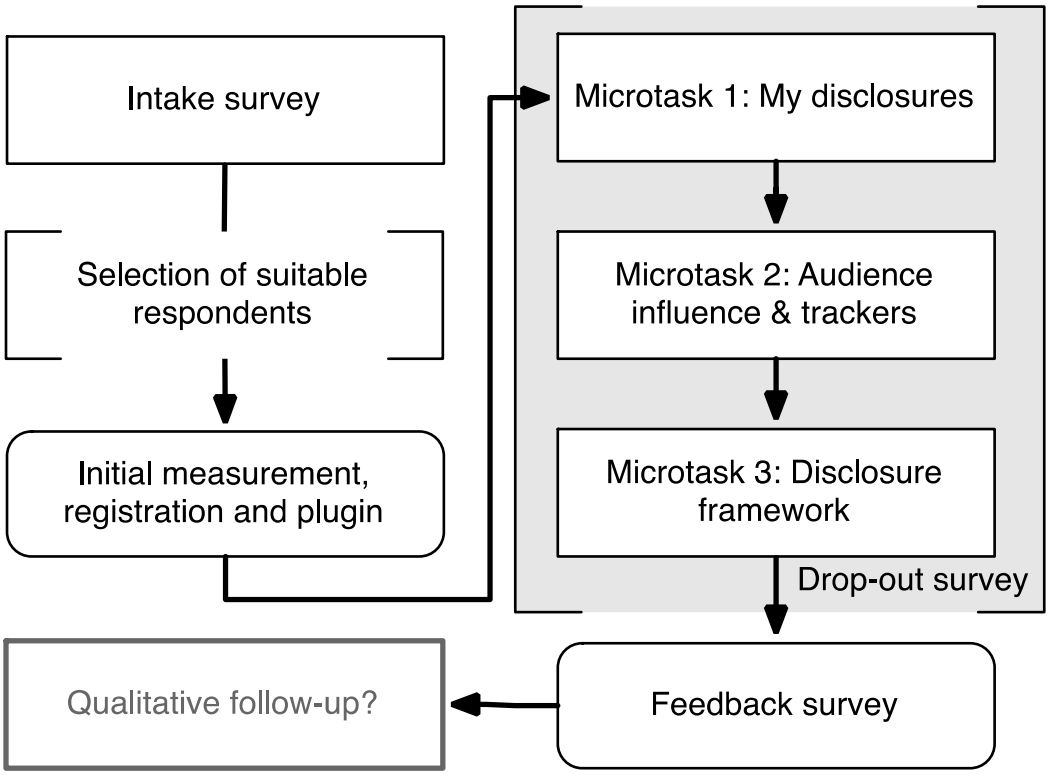

Figure 1:Living lab stepsfor the second round of pilots

And this resulted in the following time plan:

Date	**Action**	
27-30 May	Intake survey	
31 May-3 June	Initial measurement, registration and installment of plugin	
6-12 June	Microtask 1	My disclosures
13-19 June	Microtask 2	Audience influence & trackers
20-26 June	Microtask 3	Disclosure scoring framework
27-30 June	Feedback	

Table 2: Proposed timing

iMinds	LTU	Action		iMinds Respondents	LTU Respondents
09 June	**27 June**	Intake survey		221	118
14 June	**01 July**	Initial measurement, registration and installment of plugin		185	86
05 July	**06 July**	Microtask 1	My disclosures	112	53
05 July		Microtask 2	Audience influence & trackers	112	34
04 August	**11 July**	Microtask 3	Disclosure scoring framework	67	31
10 August	**16 July**	Feedback		36	27

Table 3: Actual timing

The proposed timing was not followed due to technical issues. In fact, iMinds paused their living lab to allow stability improvements in the second half of July (nevertheless, the technical improvements were effective and it was possible to resume the pilots without further problems). This explains why iMinds' timing is so different from LTU's. In both cases though, the technical issues - particularly in the first steps of the pilots - caused challenges for the respondents and this explains the drop-out.

2.1 Participants' selection criteria and intake survey

The participant selection criteria in the second round of pilots were the same as in the first round of pilots. In this section we briefly repeat them. More particularly, in both living labs, we sampled participants aiming at maximum variation for the variables age, gender and education. Additionally, the following were required criteria for selecting a participant:

- Have a Facebook account
- Have internet access at home
- Be willing to share Facebook data with our DataBait tool
- Understand: Dutch, Swedish or English
- Have to use a browser compatible with our tool (Chrome or Firefox)

The total number of respondents is aimed to be 80-100 in total. This means that if possible, we want to double the number of participants compared to the previous pilot for both living labs.

Before we sent out the intake survey (see Annex 2), we sent out an invitation (Annex 1), which informed respondents that USEMP is a project that aims to increase awareness about:

- What respondents share via Facebook
- What respondents implicitly share via Facebook, i.e. information that can be inferred from shared data

- With whom they automatically share data through cookies

The iMinds Living Lab added an incentive of 10 euros for an online shopping site if respondents complete all the tasks.

The participants from Sweden were selected through the **LTU living lab** database and from a public announcement to the university web site. In return for participation, LTU prsents them a gift card of value 150SEK (~15 euros).

2.2 Initial measurement

We identified the following objectives for the initial measurement:

- Find out what PETs they have been using the last year
- Find out how confident they are in using these PETs and other means to manage their information disclosure towards third parties on Facebook (with a focus on the things we can visualise in DataBait)
- Are respondents able to understand what they are disclosing to third parties?
    - Is this actionable information or not?
    - What were past decisions with regard to third party disclosure?
- What is the general privacy concern of our respondents?

This leads to the following survey questions:

Institutional Privacy Concern
Indicate the extent to which you are concerned about the following: (1: Not at all concerned – 5: Very concerned)(Dinev & Hart, 2004)

1: I am concerned that the information I submit on the Internet could be misused.
2: I am concerned that a person can find private information about me on the Internet.
3: I am concerned about submitting information on the Internet, because of what others might do with it.
4: I am concerned about submitting information on the Internet, because it could be used in a way I did not foresee

Indicate the extent to which you agree about the following: {Likert scale (1: Strongly Disagree; 4: Neutral; 7: Strongly Agree)}.(Krasnova, Günther, Spiekermann, & Koroleva, 2009)

Collection of information by Facebook
5: It never actually worries me that Facebook could collect information about me over the years
6: I am often concerned that Facebook could store my information for the next couple of years
7: Every now and then I feel anxious that Facebook might know too much about me

Secondary Use by Facebook
8: I am often concerned that Facebook could share the information I provide with other parties (e.g. marketing, HR or government agencies)

9: It rarely worries me that Facebook could use the information I provide for commercial purposes
10: Even if Facebook would start to share some of my information, I do not see a real threat to my privacy

2.2.1 Are respondents able to understand what they are disclosing to third parties?

The Pew Research Center(“Topline,” 2015) survey questions reflect on the decision making process with regard to disclosing personal information to third parties. It maps the effort required to understand the information provided, whether the information is confusing, how confident people are in understanding what is shared, and whether they had time to act on the provided information or not. Lastly, it probes with an open question to find an example of when respondents thought about disclosure to a third party.

The following questions were first asked, respondents can answer with yes, noor abstain from answering.

At any point, have you felt:

1. Discouraged with the amount of effort needed to understand what would be done with your data?
2. Confused by the information provided in a privacy policy?
3. Confident that you understood what would be done with your data?
4. Impatient because you wanted to learn more but needed to make a decision right away?

Next, PEW followed up with an open question that may also help in our case:

5. Could you please give us an example of a recent time where you considered whether or not to share information about yourself in return for something? What did you decide and why?

These open-ended questions aid in understanding the trade-offs respondents face when disclosing personal information towards third parties. This is important because it presents a context that usually shows that privacy is either outweighed by a benefit or outweighs a benefit. For instance, some possible answers could be:

- An Internet site was asking for control of my computer’s camera. I refused. They would have access to my personal space.
- My car insurance offered discounts for the ability to monitor my driving. I felt it was too invasive.
- Posting of resume online for job search. Needed for visibility to employers, but also risked being available for marketers, etc. My choice was between limited exposure of information and consequently limited [job-hiring] potential vs. full exposure and greater potential. I chose to post. (Rainie, 2015)

2.2.2 Experience with regard to possible solutions

Since, DataBait is a PET, it is most likely that our respondents used other PETs as well. In order to gauge their usage we created a list of PETs that manage users' social media and online digital footprint.

Please indicate whether you performed this action during the last year and how confident you were in performing this task:

- Using an app to block online third party trackers
- Using an ad blocker to stop seeing advertisements
- Visiting an opt-out platform to stop third party behavioural advertising (youronlinechoices.eu)
- Using an advertising preferences menu such as the likes offered by Google or Facebook to change or delete my ad preferences profile
- Deleting content I put on social media
- Deleting content about you someone else put on social media
- Erasing search results from Google that mention my name
- I can change the audience of Facebook content
- I know how to delete my Facebook account
- I have used the do-not-track feature in my browser settings
- I have deleted cookies through my browser

There were two answer modalities. First yes or no questions and a 7 point likert scale ranging from not confident at all to very confident. The list of solutions is based on the options offered by Facebook, other online PETs and other organisations such as Google and online advertisers.

In order to help CERTH with the development of the collection-based classifiers (one of the inference modules that work with the disclosure scoring framework), we have also asked participants to provide us with some of their personal information. This data, in conjuction with the users' OSN data is used to train the collection-based classifiers (for more details please see D6.5). This was also done in the pre-pilots (c.f. D4.2) and has been repeated here in order to obtain a larger training dataset. However, compared to the pre-pilots, we now kept the questions slightly shorter than the original version so that the participants are not discouraged to respond (see Annex 6).

2.3 Micro tasks

The overall approach is similar to the pre-pilot (D8.2) and the first pilot (D8.3); each feature was evaluated by respondents. Their evaluation would involve one of the following or a combination of more than one variable:

Usability

- How easy or difficult was this task? (1 = very hard, 7 = very easy)
- How confident are you that you fulfilled this task successfully? (1 = I am not confident at all, 7 = I am very confident)
- [Open question] If you experienced issues during the registration process you can describe them here. Feel free to suggest how we could solve this issue in the future.

Privacy concern

- [Open question] Could you please elaborate when you considered whether or not to share information about yourself during the registration process? What did you decide and why?
- If information is being gathered or profiled, ask this scale per DataBait component
    - When you see the information DataBait reveals about you, how much would you worry if X has access to this information? (1 = very worried, 7 = not worried at all) [Where X is one of Facebook friends, Facebook, Facebook's other companies, State security, advertisers, insurance company]

Evaluation of additional information

- How useful was this information in understanding what this data means? (1 = Not useful at all, 7 = very useful)
- How likely are you going to use this information if you would change something? (1 = very unlikely, 7 = very likely)

Accuracy of DataBait results[2]

- In general, how accurate is the information provided for your whole image collection? (1 =not accurate at all, 7 = very accurate)
- In general, how accurate is the information provided for a single image? (1 =not accurate at all, 7 = very accurate, Uncertain)
- How easy or difficult was this information to understand? (1 = very hard, 7 = very easy)
- [Open question] If you experienced issues with regard to the provided information, describe them here. Feel free to suggest how we could solve this issue in the future.

Time spent reading or using a component of Databait

In a few cases, we wish to log how long a reading assignment or task took. In these cases we have logged the time.

An overview of each component and the variables we ask is presented in the Table below:

DataBait component	**Usability**	**Privacy**	**Extra information**	**Accuracy of results**	**Time spent**	**Explain what actions users should perform**
Registration						
Registration	No	No	No	No	No	Register as outlined in previous pilots
DLA	No	No	Yes	No	Yes	Read

[2]Note that similar questions were asked for other DataBait components.

Summarised DLA	No	No	Yes	No	Yes	Read
Disclaimer	No	No	Yes	No	No	Read
My disclosures						
Photo insights	Yes	Yes	No	Yes	No	Browse through pictures and provide feedback on 20 depending on if the pictures depict sensitive content or not
Location insights	No	Yes	No	Yes	No	Have a look
Brands insights	No	Yes	No	Yes	No	Have a look
Additional information	No	No	Yes	No	No	Read
Audience influence						
Most influenced friends	No	Yes	Yes	Yes	No	If this information is new to them
Detailed interactions	No	No	No	Yes	No	Explore interactions by clicking on bubbles
Statistical data	No	No	No	No	No	None
Additional information	No	Yes	Yes	No	No	Read
Your disclosure scoring						
Explore the dimensions and attributes	Yes	Yes	No	Yes	Yes	Check what information could be gathered from their FB data
Change the sensitivity	Yes	Yes	No	Yes	No	Observe how disclosure scores change as the sensitivity changes
Control	Yes	Yes	Maybe	Yes	No	Examine the list of liked pages with impact on the

assistance / suggestions						disclosure a certain sensitive dimension
Additional information	No	No	Yes	No	No	Read

2.4 Registration

In this section we summarise the method that we use to compare the summarised Data Lincese Agreement (DLA) with its longer counterpart. The goal of this comparison was to see if it made sense to show users of DataBait a shortened version of the DLA or not. For this to be true, we compared ease of use, understanding and time taken to go through the DLA exercise.

Both living labs divided their respondents in an A and B group, which both received a different DLA as part of the initial measurement survey. The DLA had to be part of the surveys in order to log the time required to complete the survey. Both DLAs can be found in Annex 7.

2.4.1 Questions after both DLAs

After the respectiveDLA sections, we asked our participants the following questions:

Usability

- How easy or difficult was this task? (1 = very hard, 7 = very easy)
- How confident are you that you fulfilled this task successfully? (1 = I am not confident at all, 7 = I am very confident)
- [Open question] If you experienced issues during the registration process you can describe them here. Feel free to suggest how we could solve this issue in the future.

Evaluation of extra information

- How easy or difficult was this information to understand? (1 = very hard, 7 = very easy)
- [Open question] If you experienced issues with regard to the provided information, describe them here. Feel free to suggest how we could solve this issue in the future.

Evaluation of understanding

Please answer the following questions with regard to the Data License Agreement:

- For which purpose do you allow us to use this data? (Scientific purpose)
- Did you give us your explicit consent? (Yes)
- When will we delete your data? (Within three months after the end of the project)
- With whom did you sign this contract? (USEMP consortium partners)
- Did you agree to let us process sensitive data with regard to your health or sex life? (Yes)

2.5 Microtask 1: My disclosures

We already outlined the general questions for each microtask, so we will only elaborate on additional questions. For each task this will consist of their additional information or if new components were added, questions about these new components.

2.5.1 Location insights

With regard to Location insights, the only thing we added, compared to the previous pilot, was additional information. This was presented after users finished the microtask.

Additional information:
The locations you see in this page are the result of an automatic location estimation algorithm that processes the text content of your posts and tries to predict the location where these posts refer to or the location indicated in Facebook.

This means that this algorithm presents you with an overview of all locations you mentioned in posts, either through check-ins or by referring to them.

If you are not happy with disclosing a particular location, there are several things you can do.

1. ***When should you consider changing the visibility or delete a location?***
   If you do not want a person or party to know you have been here. For example, you disclosed your home address, a location that might negatively impact your safety or a location that diminishes the chances at being offered a job. Or because you have never been there and the information on Facebook portrays this wrongly.
2. ***You do not want this location to be seen by certain friends on Facebook?***
   In this case, you should visit your Facebook profile and click on the activity log, shown on the right of your profile picture.
   Here you can use the search box to find that particular post and change its visibility.
3. ***You want no reference to this location at all?***
   In this case, you should visit your Facebook profile and click on the activity log, shown on the right of your profile picture.
   Here you can use the search box to find that particular post and delete it.

We asked the following questions related to this additional information:

We would like to ask you some questions with regard to this information

- How easy or difficult was this information to understand? (1 = very hard, 7 = very easy)
- How likely are you going to use this information if you would want to adjust something? (1 = very unlikely, 7 = very likely)
- [Open question] If you experienced issues with regard to the provided information, describe them here. Feel free to suggest how we could solve this issue in the future.

2.6 Microtask 2: Photo insights

In Photo insights, a new component was added to see what pictures DataBait deemed sensitive. This feature was used to inform users but also to allow them to improve the accuracy of the algorithm by providing feedback with regard to the sensitivity of a picture, their privacy setting and the concepts associated with the image.

In order to provide feedback, we gave participants the following instructions:

After you had a look, please finish the following task.

1. *Click on concepts which are either displayed in the grey box or displayed as the Top 20 visual concepts in bubbles.*
2. *If you click on a concept you will see pictures that have a green or red border. This is an **estimation** (made by DataBait) of whether this image is **sensitive-red** (i.e. most users would share it only with close friends of facebook) or **less sensitive-green** (i.e. most users would share it with all their friends on facebook)..*
3. *Click on a picture and review the information provided there. More specifically, we want you to do two things:*
    a. *Give us your feedback on the following two questions:*
        i. *What is your preferred audience setting?*
        ii. *What kind of personal information is revealed in this image, according to you?*
    b. *Check if the image is currently shared with a larger audience that you would like to. If so, you can follow the link to this image on Facebook where you can change its privacy settings. To help you identify such images, besides the sensitive/less-sensitive prediction, on the right side of the image we provide an indication of the image's current privacy settings on Facebook (note that due to limitations of Facebook's API this might not always be accurate).*
4. *Repeat this for at least 20 pictures so that we teach our algorithms to recognize sensitive images even better. Please give your feedback on images from a range of concepts.*

Next we asked respondents the same questions with regard to usability, accuracy and privacy.

Additional information
The tag cloud you see on this page illustrates a profile that can be automatically inferred by DataBait from the images that you posted on Facebook. DataBait predicts tags from a set of over 17,000 visual concepts following a procedure that is described in more detail here

The tag cloud shows the identified concepts with a size proportional to their frequency in the posted online social network images.

What does this information mean?
It means that beside the audience you specified, apps, Facebook and its family of companies may derive the same information (according to our DataBait algorithms (see DataBait disclaimer) if they use similar algorithms.)

You do not want this image to be seen by certain friends on Facebook?
If this is the case, you can change the settings of any particular photo on DataBait by clicking on this image and selecting a new audience in Facebook's interface.

You want nobody to see this image?

If you decide that nobody may see this image, click on the image and subsequently click on the link that brings you to Facebook. Now click on options. Here two things may happen, if you uploaded the picture, you can delete it directly by selecting delete. If you did not delete the picture, you may choose to report the image or contact the uploader to ask him or her to delete it.

This section was followed by the same questions with regard to additional information.

2.6.1 Brands insights

For Brands insights we used the same template as Photo insights, as a result, it is not repeated here.

2.6.2 Audience influence

For Audience influence, we asked about accuracy and privacy and provided the following additional information:

Additional information
Databait processes the data you have shared in Facebook and then computes who interacted the most with your shared data.

It is possible to review specific interactions by clicking on detailed interactions and then clicking on particular bubbles, which will bring you to that specific interaction on Facebook.

What does this mean?
DataBait presents you with a visualization that depicts which of your friends interacted with what you shared on Facebook. Depending on the visualization, the volume of the bubble or the amount of coloured bubbles inform you of the degree of interaction. The larger the bubble of a profile picture, or the more coloured bubbles, the more somebody interacted with your content.

How to change the visibility?
If this is the case, you can change the settings of any particular interaction by clicking on this interaction and selecting a new audience within Facebook's interface.

How to delete an interaction?
If you decide that nobody may see this image, click on the image and subsequently click on the link that brings you to Facebook. Now click on options. Here two things may happen, if you uploaded the picture, you can delete it directly by selecting delete. If you did not delete the picture, you may choose to report the image or contact the uploader to ask him or her to delete it.

2.7 Microtask 3: Disclosure Scoring Framework

In this section we summarise the procedure we followed to evaluate a new DataBait feature, the disclosure scoring framework. The disclosure scoring framework has been briefly described in Chapter 1 but - for clarity - we repeat the basic idea here. The main function of the disclosure scoring framework is to provide an overview of the different types of information

that the user discloses to the OSN, either explicitly or implicitly. Importantly, different aspects of the disclosed information are expressed through a number of scores (visibility, sensitivity, etc.), the most important of which is the overall disclosure score that quantifies the risk associated with the disclosure of some specific type of information. Moreover, the disclosure scoring framework is based on a number of inference modules that analyze the user's OSN data and feed their results into the scoring framework. Additionally, the scoring framework works closely with a sub-module that assists the user to better control their OSN presence by suggesting to them to reconsider sharing pieces of content that have a high contribution to the user's disclosure score. For more details please see D6.5.
Users were instructed to go to this feature and explore it after reading the additional information provided as a part of DataBait's interface. Next they answered the questions which can be found in Annex 8 because they are too lengthy to discuss here.

2.8 Feedback survey

In the feedback survey we asked the same questions included in the initial measurement but we have also added an extra question. A general usability scale, that was also used in D8.2-3, so that we can compare results and have an indication of the general usability of DataBait.

Since iMinds' living lab evaluation ended much later than LTU's, we have also added an extra question requested by the consortium. In light of the ending of the project, we as a consortium wanted to know what features should be prioritised if DataBait development would continue within other projects.

System Usability Scale:

Indicate your agreement with the statements provided below with a likert scale:

1. I think that I would like to use DataBait frequently
2. I found DataBait unnecessarily complex
3. I thought DataBait was easy to use
4. I think that I would need the support of a technical person to be able to use this tool
5. I found the various functions in DataBait very well integrated
6. I thought there was too much inconsistency in DataBait
7. I imagine that most people would learn to use this tool very quickly
8. I found DataBait very awkward to use
9. I felt very confident using DataBait
10. I needed to learn a lot of things before I could get going with DataBait

Privacy concern

Indicate the extent to which you are concerned about the following: (1: Not at all concerned – 5: Very concerned)

1. I am concerned that the information I submit on the Internet could be misused.
2. I am concerned that a person can find private information about me on the Internet.
3. I am concerned about submitting information on the Internet, because of what others might do with it (like same analysis with DataBait).
4. I am concerned about submitting information on the Internet, because it could be used in a way I did not foresee
5. I am concerned if Facebook could do the same analysis like DataBait with my profile. (new question)

Indicate the extent to which you agree about the following: (Likert scale (1: Strongly Disagree; 4: Neutral; 7: Strongly Agree)).

Collection of information by Facebook

6. It never actually worries me that Facebook could collect information about me over the years
7. I am often concerned that Facebook could store my information for the next couple of years
8. Every now and then I feel anxious that Facebook might know too much about me (like private categories in DataBait) (modified question)

Secondary Use by Facebook

9. I am concerned that Facebook could share the result of their analysis (e.g. such as DataBait) on my profile with other parties (e.g. marketing, HR, or government agencies) (modified question)
10. I am often concerned that Facebook could share the information I provide with other parties (e.g. marketing, HR or government agencies)
11. It rarely worries me that Facebook could use the information I provide (e.g. same done by DataBait) for commercial purposes (modified question)
12. Even if Facebook would start to share some of my information, I do not see a real threat to my privacy
13. It does not worry me if Facebook would use my least interesting privacy category for commercial purposes (new question)
14. It would not bother me if Facebook asks me to choose what privacy category would be used for commercial purposes New question
15. I feel Facebook should ask me to choose what privacy category would be shared with other parties (e.g. marketing, HR, or government agencies) (new question)

DataBait prioritisation exercise

Pilot participants were asked to prioritise what DataBait functions they found most important by giving the most important function a 1 and the least important a 7. The following components were compared:

- Location insights
- Photo insights
- Brand insights
- Visualization of your audience
- Historical data
- Your disclosure scoring
- Trackers

3 Reporting

In this part we report on the results in the following order. We start by giving an overview of the respondents' demographic information, as well as their attitudes and practices towards disclosure of information. Next, we will review the results of the initial measurement, followed by the rest of the proposed living lab outset as outlined in Figure 1 (p. 6). Note that the interview

insights have been embedded in the feedback related to each living lab step and will not be treated separately.

3.1 Respondent overview

Here we report on the distribution of our participants' gender, **age**, **education** and **use of Facebook**. Also, we mention how respondents feel about sharing data with third parties in general. These results come from the intake and initial measurement survey and we look at the Belgian and Swedish participants independently.

3.1.1 Demographic information of Belgian participants

iMinds' respondents were very similar in terms of gender; education and Facebook use compared to the previous pilot. As mentioned in the participant selection method section, participants were selected from the same large panel and respondents of previous DataBait pilots were invited again to join this pilot. Opposite to the Swedish sample, the Belgian sample had more male than female participants.

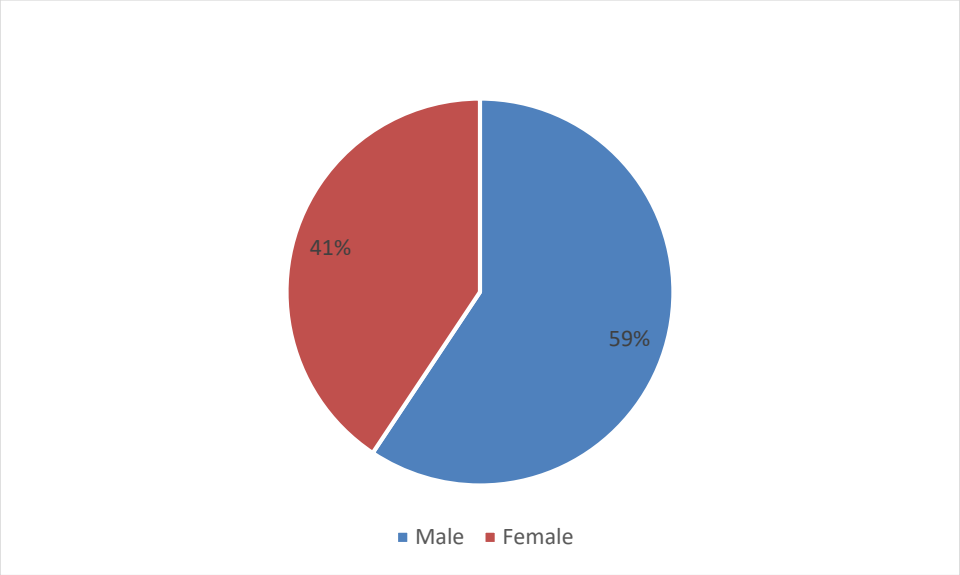

Figure 2: Gender (%, iMinds n=187)

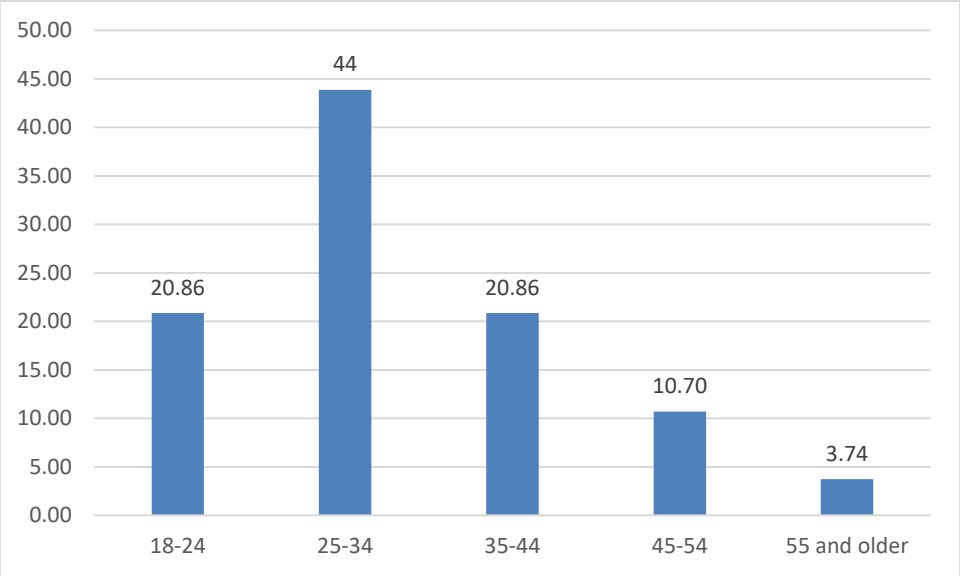

Figure 3: Age category (%, iMinds n=187)

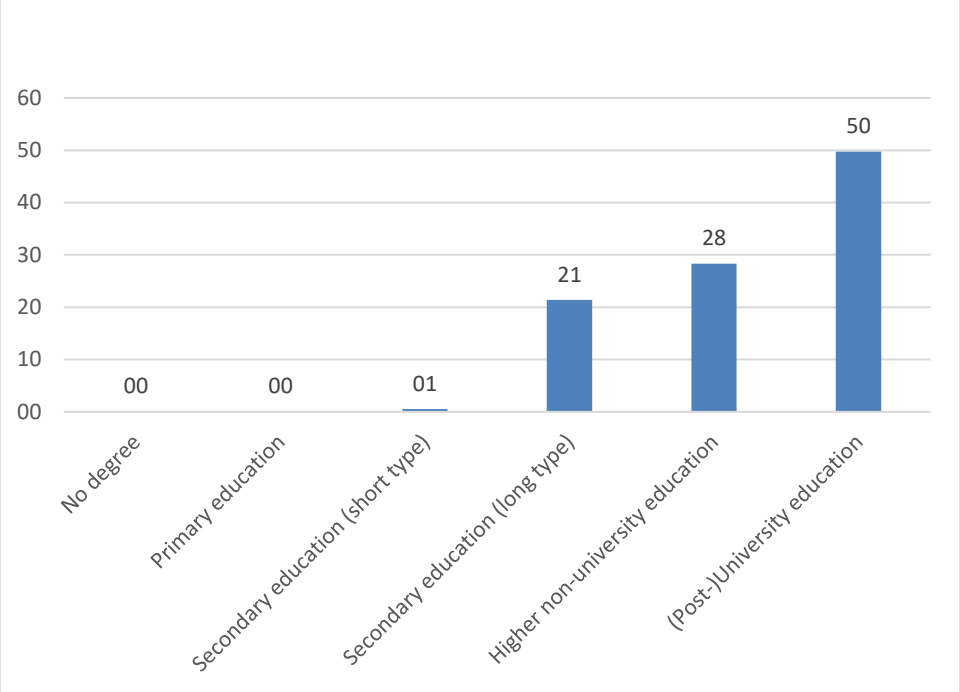

Figure 4: Education (%, iMinds n=187)

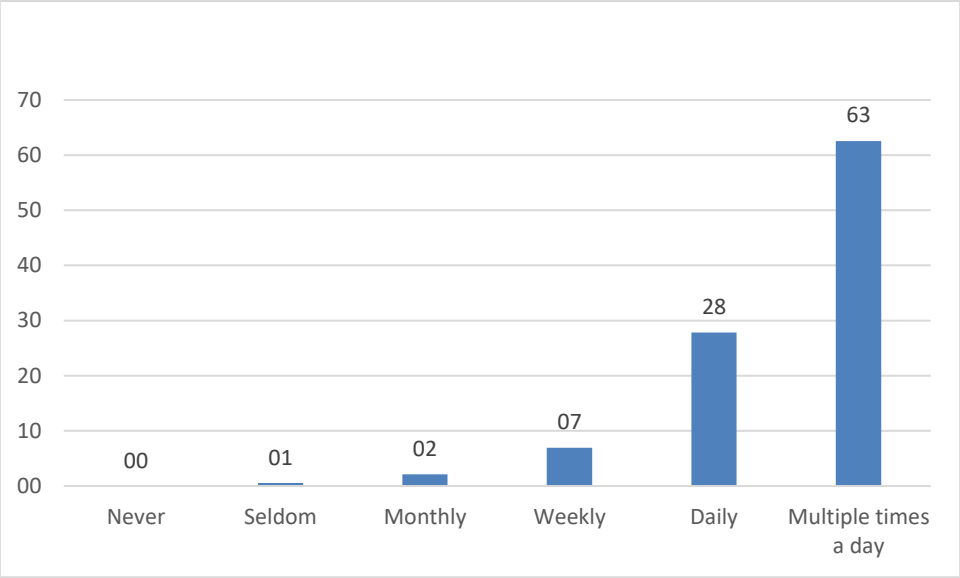

Figure 5: Facebook use (%, iMinds n=187)

3.1.2 Demographic information of Swedish participants

LTU recruited participants through an invitation advertised in the LTU website for both employees and students. We also invited users in the previous pilot held during March 2016 that showed interest to take part in the current pilot study. There were also invitations posted on all Swedish universities and other public Facebook pages. A total of 118 users showed their interest and completely filled out the intake survey. Please note that not all participants finished all of the tasks due to some technical problems as mentioned in the first chapter and as will be further discussed in a later section. Female participants were dominating by 52%.

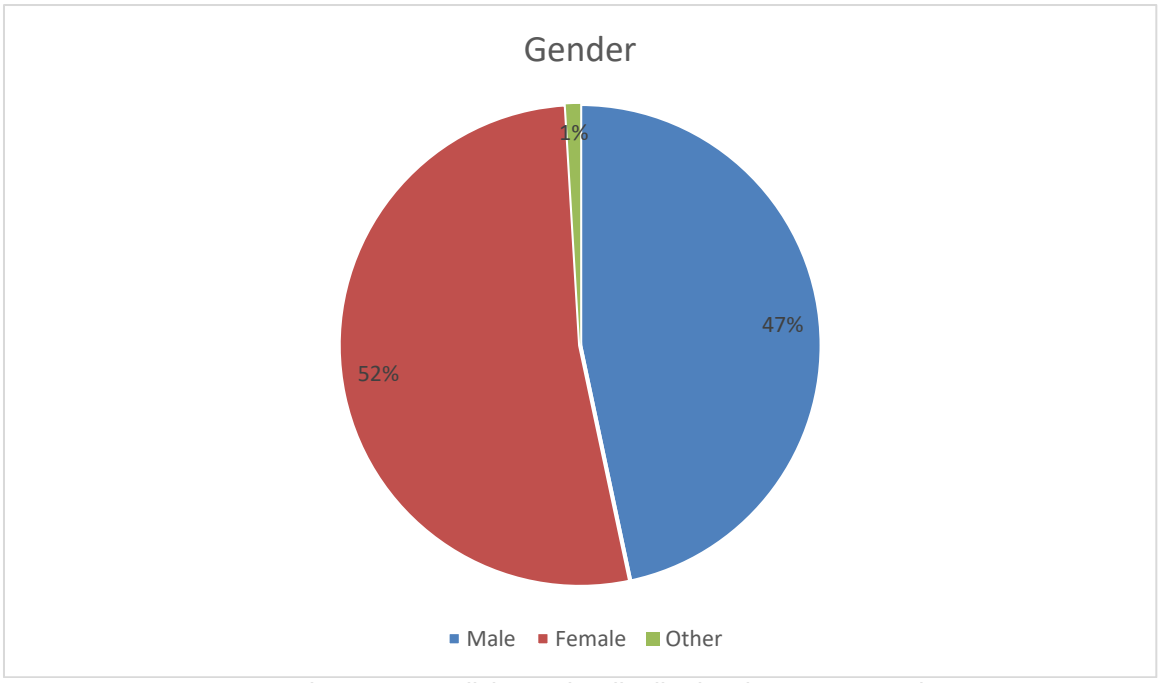

Figure 6: Swedish gender distribution (%, LTU n=118)

From an age perspective, most participants were young adults between18 and 34 years old (72% of the whole number of respondents). Figure 7 demonstrates the age distribution of the Swedish study.

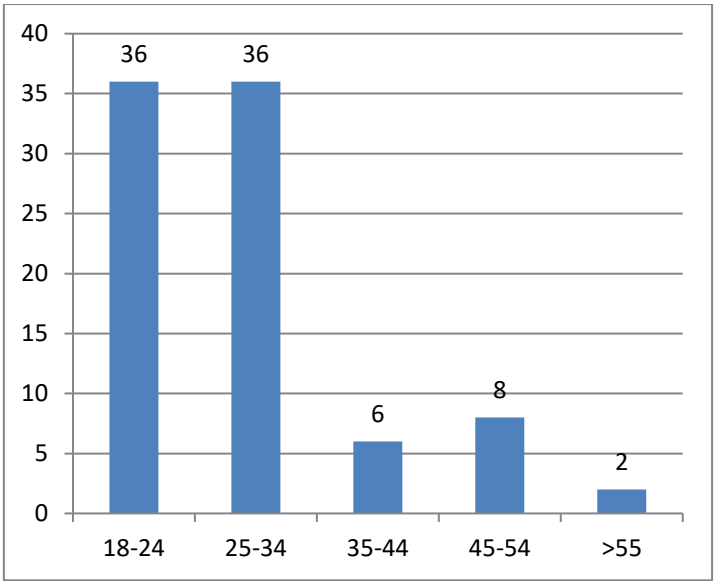

Figure 7: Age distribution of Swedish participants (%, LTU n=118)

Regarding the level of education, Swedish participants were almost equally divided into those who were university students (49%) and those with minimum university education (48%) (Figure 8).

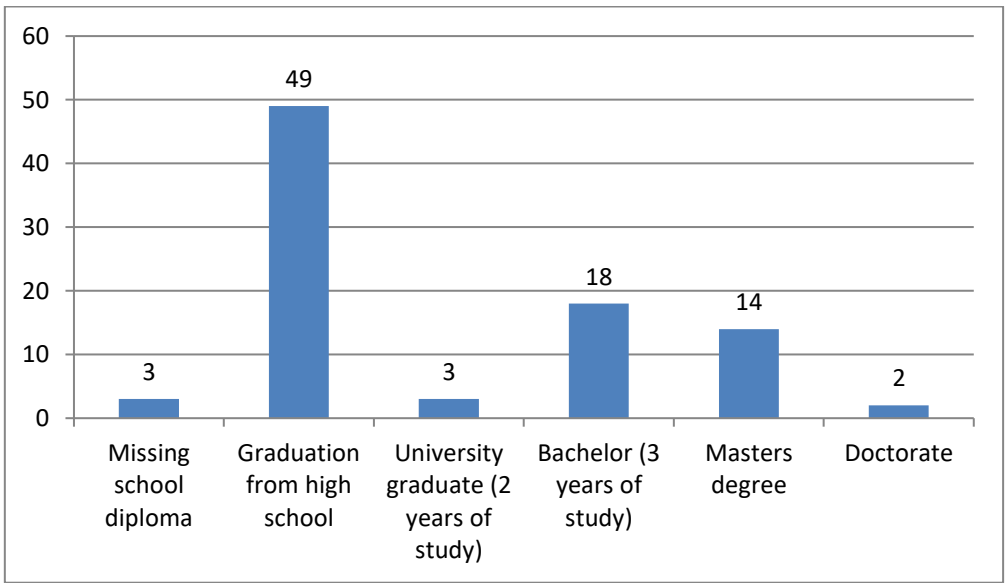

Figure 8: Swedish participants' minimum education level (%, LTU n=118)

Figure 8 shows the usage of Facebook by the respondents. More than half of the participants check and use Facebook several times a day, while it could be said that 86% are active Facebook users.

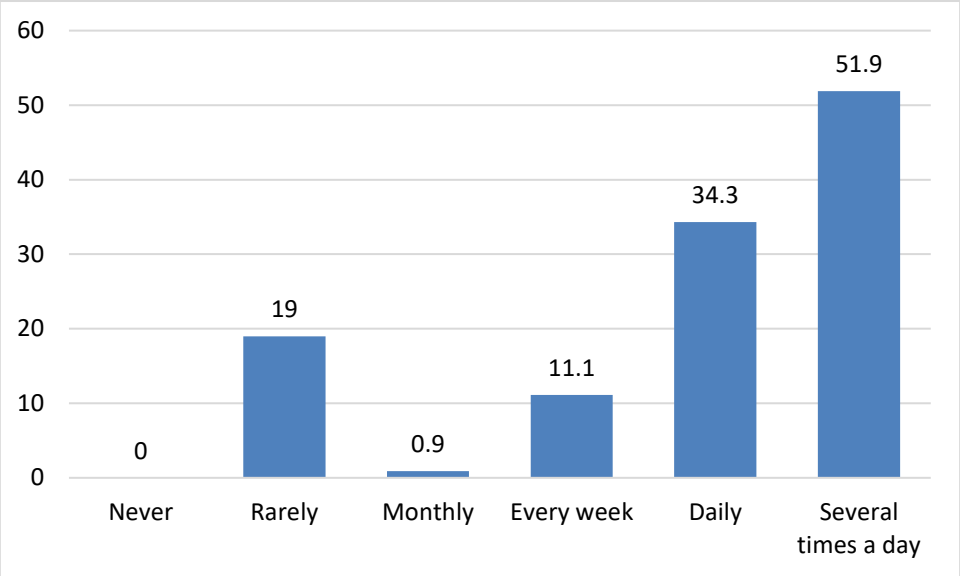

Figure 9: Swedish participants' Facebook use (%, LTU n=118)

3.1.3 Initial measurement

As described in the second chapter, in the initial measurement we asked the participants about the following: their concern toward institutional privacy, their understanding of disclosure to third parties and their experience with regard to PETs.

With regard to institutional privacy, respondents are somewhat concerned about the way their information is collected online. The most interesting aspect is that users are worried about the way they disclose information that they do not forsee. In Table 4 around 62% of the Swedish participants were highly concerned about the collection of information which could be used beyond their expectations.

LTU's institutional privacy concern:

	LTU
I am concerned that the information I submit on the Internet could be misused.	3,37
I am concerned that a person can find private information about me on the Internet.	3,32
I am concerned about submitting information on the Internet, because of what others might do with it.	3,50
I am concerned about submitting information on the Internet, because it could be used in a way I did not foresee	3,65

Table 4: Institutional Privacy concerns Indicate the extent to which you are concerned about the following (1= Not at all concerned, 5= very concerned) (LTU N=92)

When we turned our focus in the questionnaire towards Facebook's way of handling users' privacy, some interesting results were found. Respondents replied that they do care about their historical data being collected and stored by Facebook. Also, the most interesting finding: that the shared contents in Facebook are valuable for the company in terms of secondary purposes such that selling to third parties. However, they feel somehow safe that their information is

being held by Facebook only. In deliverables D8.2 and D8.3, this was explained by trust of end users towards Facebook; however, this is the case only if the data stays in Facebook and not shared over to the third parties. All in all, the mean score of the level of concern over the collection and secondary use of users' information by Facebook is in the neutral level, highlighting the respondents' low awareness of the institutional privacy practices. Table 4 summarizes the results.

	LTU
It never actually worries me that Facebook could collect information about me over the years	3,46
I am often concerned that Facebook could store my information for the next couple of years	4,51
Every now and then I feel anxious that Facebook might know too much about me	4,57
I am often concerned that Facebook could share the information I provide with other parties (e.g. marketing, HR or government agencies)	4,66
It rarely worries me that Facebook could use the information I provide for commercial purposes	3,74
Even if Facebook would start to share some of my information, I do not see a real threat to my privacy	3,53

Table 5: Institutional Privacy concerns: Indicate the extent to which you agree about the following (1= strongly disagree, 7= strongly agree) (LTU N=91)

iMinds' results about institutional privacy concern are summarized in Table 6. Threats from third parties collecting and using personal information resulted in expressing most of the concerns over the adverse effects of sharing personal information online. 68% of the users agreed that keeping privacy intact from online companies is important. One concern over online privacy is the way personal information is handled by companies and 53% of the respondents showed their concern in this respect. Participants in the questionaire also expressed their overall importance of online privacy and they believe that other people have been also thinking the same.

	Strongly disagree	**Disagree**	**Somewhat disagree**	**Neutral**	**Somewhat agree**	**Agree**	**Strongly agree**
All things considered, the Internet would cause serious privacy problems.	0,00	2,17	6,52	2,17	28,26	32,61	28,26
Compared to others, I am more sensitive about the way online companies handle my personal information.	2,13	8,51	12,77	23,40	17,02	31,91	4,26
To me, it is the most important thing to keep	0,00	2,13	6,38	23,40	23,40	40,43	4,26

my privacy intact from online companies.							
I believe other people are too much concerned with online privacy issues.	10,64	14,89	29,79	17,02	21,28	4,26	2,13
Compared with other subjects on my mind, personal privacy is very important.	2,08	4,17	14,58	33,33	31,25	12,50	2,08
I am concerned about threats to my personal privacy today.	4,17	6,25	12,50	20,83	31,25	18,75	6,25

Table 6: Institutional privacy (%, iMinds n=157)

Respondent's understanding of disclosure to third parties is presented inTable 7. The result from the second pilot is identical to the result of the first pilot with no sensible deviation. On average, respondents, feel that the privacy policies are confusing and have low confidence in understanding the collection and use of their personal information over the Internet.

	iMinds (mean)	**LTU (mean)**
Discouraged with the amount of effort needed to understand what would be done with your data?	4,40	4,45
Confused by the information provided in a privacy policy?	4,94	5,49
Confident that you understood what would be done with your data?	3,38	2,58
Impatient because you wanted to learn more but needed to make a decision right away?	4,46	3,99

Table 7: Disclosing information to third parties in general "At any point, have you felt …?" (1= strongly disagree, 7= strongly agree) (iMinds n=157, LTU n=91)

Short summary of most interesting remarks with regard to the open question:

Our respondents also had to provide an example where they decided to disclose or keep data form a third party. In these cases, respondents reflected on general rules with regard to disclosing information online, decisions to share data and decisions not to share data. For example how they were doubting to enter a game or contest if it asked for data that did not seem relevant for the game or contest.

Use of PETs

We asked participants about the ways in which they manage their privacy. In terms of automatic approaches like PETs, there is a low percentage of adoption. But ad blockers are an exception, as these are used by a majority in the two living labs. However, they seem to be more in favor of manual approaches like deleting contents from OSN (~46%), changing Facebook settings to limit their audience (~70%) and deleting cookies from their browsers (~64%). Regarding the collection of use of information over the internet, the general strategies

seem to be not practiced, like opting out or ad preferences settings.

PET usage	iMinds	LTU
Using an app to block online third party trackers	29,79	29,67
Using an ad blocker to stop seeing advertisements	74,47	63,74
Visiting an opt-out platform to stop third party behavioural advertising (youronlinechoices.eu)	10,64	8,79
Using an advertising preferences menu such as the likes offered by Google or Facebook to change or delete my ad preferences profile	25,53	35,16
Deleting content I put on social media	63,83	69,23
Deleting content about you someone else put on social media	46,81	45,05
Erasing search results from Google that mention my name	8,51	18,68
I can change the audience of Facebook content	80,85	57,14
I have used the do-not-track feature in my browser settings	29,79	40,66
I have deleted cookies through my browser	59,57	67,03
None of the above	0,00	N/A

Table 8: Please tell us whether you did one of these activities in the past year and how confident you are in performing this activity (LTU n=91)

In overall, by comparing the results obtained during the second pilots with those of the first pilot, there was no clear deviation from the initial measurement of privacy. Respondents are generally reluctant to take actions enhancing their privacy as a result of low awareness of what happens with their online information.

3.2 Registration

We tried to test the two versions of the DLA by providing an A/B test to our respondents in which we compared on the following: time taken, understanding, usability, quality of the provided information.

	iMinds		LTU	
How easy or difficult was the DLA?	Short	Long	Short	Long
Very difficult	7,41	5,19	0	9,38
Difficult	2,47	2,60	5,13	15,63
Rather difficult	9,88	6,49	10,26	21,88
Neutral	8,64	14,29	12,82	25
Rather easy	22,22	23,38	28,21	9,38
Easy	22,22	24,68	7,69	9,38
Very easy	27,16	23,38	35,9	9,38
	n=76	n=75	n=39	n=32

Table 9:DLA ease of use (%)

	iMinds		LTU	
How easy or difficult was this information to read?	Short	Long	Short	Long
Very difficult	1,32	2,67	3,13	4,35
Difficult	1,32	1,33	3,13	0
Rather difficult	7,89	10,67	15,63	4,35
Neutral	18,42	12,00	15,63	29,09
Rather easy	25,00	24,00	9,38	34,78
Easy	26,32	25,33	18,75	17,39
Very easy	19,74	24,00	34,38	13,04
	n=76	n=75	n=32	n=23

Table 10:DLA ease of reading(%)

In Table 11: DLA reading self-assessment (%), we can see that iMinds' respondents show little difference with regard to how difficult the two versions of the DLA were in general or the reading of the text was. For LTU on the other hand, a clear ease of use is indicated by respondents for both.

	iMinds		LTU	
How successful were you in reading the DLA?	Short	Long	Short	Long
Very unsuccessful	14,81	4,00	2,56	3,23
Unsuccessful	3,70	1,33	7,69	22,58
Rather unsuccessful	4,94	6,67	10,26	25,81
Neutral	6,17	5,33	17,95	16,13
Rather successful	22,22	17,33	17,95	12,9
Successful	18,52	26,67	20,51	6,45
Very successful	29,63	38,67	23,08	12,9
	n=76	n=75	n=39	n=31

Table 11: DLA reading self-assessment (%)

The same tendency can be witnessed for respondent's self-evaluation of the task. iMinds is less clear in its preference but more respondents of the long DLA deemed themselves successful. For LTU the tendency is the other way around, there is a clear positive self-evaluation for the shorter version.

Average time to finish the survey containing the summarised DLA	**iMinds**		**LTU**	
	Short	Long	Short	Long
	7,5	7,7	7,17	9,31
	n=49	n=58	N=31	N=19

Table 12: Average time to read summarized DLA (minutes)

When comparing the time it took for both DLAs, the same tendency can be noted: iMinds had very similar times, while LTU is clearer in the difference. In general, the short DLA took less time to read. These results were expected.

	iMinds	
Number of correct answers	Short	Long
0	14	16
1	11	22
2	27	20
3	17	10
4	2	3

Table 13: Number of correct answers given per respondent (iMinds, n= 140)

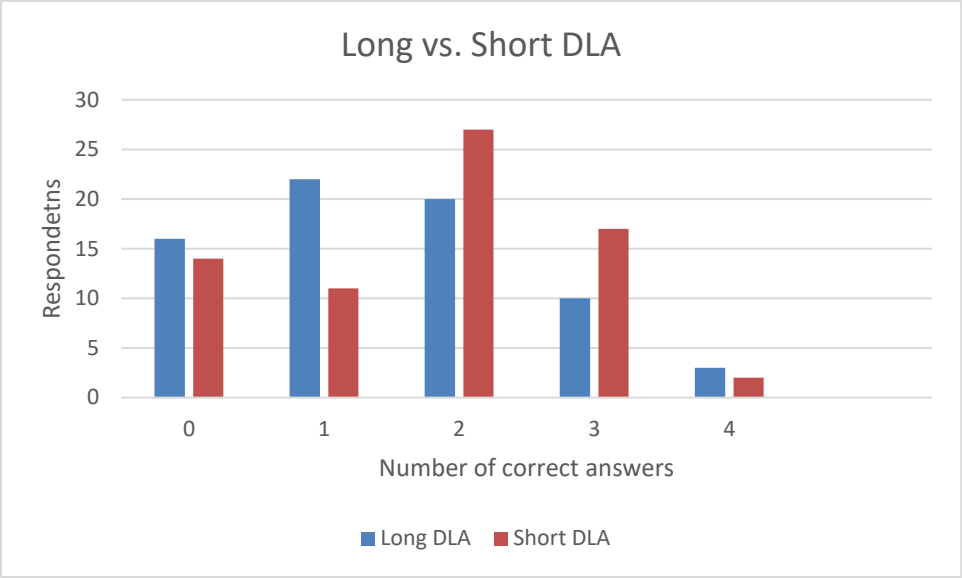

Figure 10: DLA comparison (iMinds, n= 140

Lastly, we look at the number of correct answers per respondent. Here we can see a clearer pattern. Readers of the long DLA are more prone to make mistakes than the readers of the short DLA. This means that the retention of the text is higher for the short DLA.

In the interviews, respondents were asked to compare the two versions of the DLA. Respondents were unanimous: they preferred the short DLA for the following reasons. It presents them with less text, so the task seemed less daunting. The text itself was made more readable thanks to bullets and short paragraphs. Lastly, respondents seemed to understand that this text was a summary that highlighted important information.

However, one respondent, Rita, was sceptical about the length of the summary: “How can I trust that all relevant information is in there?” And what is more, “Can this be a real privacy statement if other statements are so much longer?” This is a risk and Rita agreed that she could always read the full version if the need arose.

Recommendation

It is hardly surprising that DLAs and privacy statements should be made shorter. This increases chances that respondents read the statement and remember more information. What is more, the whole process is perceived as being easier resulting in a better self-evaluation.

Secondly, having shorter DLAs or privacy statements seems to challenge the notion of their longer counterparts: they do not have to be this long. If more and more of these short versions are implemented, they may become the norm for users because they expect the same ease of use from competitors or other online actors.

3.3 Location leaks

This feature did not change and respondents did not grade it differently from the previous pilot. As a result, the same tables are shortly reported here.

How easy or difficult was the task with regard to Location leaks?	iMinds	LTU
Very difficult	5,97	2,22
Difficult	0,00	4,44
Rather difficult	2,99	8,89
Neutral	16,42	26,67
Rather easy	14,93	31,11
Easy	22,39	13,33
Very easy	37,31	13,33
Mean score	5,51	4,73
	n= 67	n=45

Figure 11: Location privacy ease of use (%)

How accurate are the locations DataBait deduced from your posts?	iMinds
Not accurate at all	17,91
Not accurate	14,93
Neutral	28,36
Accurate	13,43
Very accurate	14,93
	n= 67

Table 14: Location accuracy iMinds (%)

How accurate are the locations DataBait deduced from your posts?	LTU
Not accurate at all	4,44
Not accurate	17,78
Somewhat not accurate	22,22
Neutral	22,22
Somewhat accurate	11,11
Accurate	8,89
Very accurate	2,22
Not-sure	11,11
Mean	3,60

	n= 45

Table 15: Location LTU (%)

3.4 Image leaks

In the second pilot, an extended feature which detects image privacy settings in Facebook was tested for the first time. The photos which the “image privacy” algorithm detects as private are shown with red outlining and the ones which are detected as public are labeled in a green outline. Since this feature was new, we asked participants to check this feature and answer a couple of questions regarding the usability and affordances of the feature. The results of each question along with their analysis is presented below.

First of all we asked the participants to check at least 20 photos in their DataBait account and report back the privacy setting of each photo. In case of the privacy settings of a private photo was larger than intended, we guided them to go to Facebook and change the setting to their desired setting.

Table 16 summarizes the results on the difficulty of this task. On average, participants found it rather easy to perform the task (mean 4.5). Moreover, the users' confidence level that they successfully fulfilled the task (mean 4.1) indicates that the feature was easy to use, as can be seen in Table 17.

How easy or difficult was the task with regard to Image leaks?	iMinds	LTU
Very difficult	16,67	4,88
Difficult	1,39	4,88
Rather difficult	9,72	9,76
Neutral	18,06	24,39
Rather easy	18,06	16,51
Easy	25,00	21,95
Very easy	11,11	14,63
Mean score	4,39	4,73
	n= 72	n=41

Table 16: Image privacy ease of use (%, n = 72 iMinds, LTU n=41)

How certain are you that you fulfilled the task successfully?	iMinds	LTU
Very uncertain	21,13	21,95
Uncertain	0,00	7,32
Rather uncertain	9,86	4,88
Neutral	14,08	14,63
Rather certain	16,90	17,07

Certain	29,58	21,95
Very certain	8,45	12,2
Mean score	4,28	4,12
	n= 71	N=41

Table 17: Image privacy self-evaluation (%, n = 71 iMinds, LTU n=41)

When it comes to the usefulness of the image privacy feature, on average, respondents were neutral (2,8) about the usefulness of the predictions but only a 10% (iMinds) and 17% (LTU) find the predictions useless (Table 19). These results are quite encouraging provided that a) there are users who might consider themselves already protected (e.g. users with very few and insensitive photos) and b) the predictions were based on a generic private image detection model which was expected to have a relatively low accuracy for some users due to its inability to capture the variation in user perceptions regarding privacy. As shown in D5.6 (section 4), the accuracy of the predictions can be significantly improved by employing a limited amount of user-feedback in order to build personalized privacy models. This increased accuracy will probably also improve users' opinion on the usefulness of the predictions.

Did you find the predictions (red/green borders) made by the tool useful?	**iMinds**	**LTU**
Not useful	10,14	17,07
Somewhat not useful	26,09	12,2
Neutral	39,13	39,02
Somewhat useful	23,19	29,27
Useful	1,45	2,44
Mean score	2,8	2,88
	n= 69	n=41

Table 18: Image privacy predictions' usability (%, n = 69 iMinds, LTU n=41)

In addition to detecting sensitive images, the extended module also presented the current privacy settings of each image on Facebook in order to facilitate easy identification of images whose actual settings are different from the predicted or the intended ones. However, as explained in D5.6 (section 4.4), Facebook's API (v2.6) provides only album-level privacy settings which are often different from the image-level ones. Despite a workaround that was implemented (see D5.6) in order to obtain image-level privacy settings, this was not possible for all photos. Thus, we asked users to access the accuracy of the text describing the current privacy settings of each image. As shown in Table 19, on average users were neutral regarding the accuracy of the descriptive text. Unfortunately, this feature cannot be improved, unless Facebook changes each API to provide image-level privacy settings.

Did you find the text describing each photo's current Facebook privacy settings accurate?	**iMinds**	**LTU**
Not accurate	14,49	9,76
Somewhat inaccurate	15,94	12,20
Neutral	36,23	46,34
Somewhat accurate	21,74	24,39

Accurate	11,59	7,32
Mean score	3,00	3,07
	n= 69	n=41

Table 19: Accuracy of privacy setting description composed based on the information returned be Facebook's API (%)

When asked whether the module helped them to identify images that were shared beyond their expectations, about 30% of the participants in LTU's living lab answered positively, while a 35% of the participants in iMinds' living lab were neutral to positive. These percentages should be considered satisfactory, if we take into account the fact that some participants might have shared only images without sensitive content or had already correctly adjusted privacy settings. In addition, there were some technical issues that were experienced during the pilots and which were highlighted by some participants, i.e. some participants could not see their photos due to slow processing speeds, at some points the server was unavailable, some people saw the message that their data was being processed constantly, a few participants saw a grey outline which was not responsive.

Did this tool help you identify photos that you had inadvertently shared with a larger than the intended audience?	**iMinds**
No	34,78
Rather no	30,43
Neutral	28,99
Rather yes	5,80
Yes	0,00
Mean score	2,06
	n= 69

Table 20: Identification of shared images with larger audience (%)

Did this tool help you identify photos that you had inadvertently shared with a larger than the intended audience?	**LTU**
No	72,50
Yes	27,50
	n=41

Table 21: Identification of shared images with larger audience (%)

Lastly, we asked respondents how concerned they would be if other parties had access to the information portrayed in Image leaks. The results show that this feature was able to raise personal awareness and users did not show much concern over institutional privacy, as portrayed in Table 22 and Table 23. Here users are more worried about access to their information by friends on Facebook rather than by any third party.

iMinds

	Very concerned	Concerned	Somewhat concerned	Neutral	Somewhat unconcerned	Unconcerned	Very unconcerned	Weighted Average
Your friends on Facebook	33,85	26,15	18,46	18,46	1,54	0	1,54	2.34
Facebook	9,23	15,38	15,38	36,92	16,92	4,62	1,54	3.57
Other Facebook companies	10,77	9,23	15,38	35,38	16,92	10,77	1,54	3.77
State security	18,46	21,54	16,92	29,23	6,15	6,15	1,54	3.08
Advertisers	12,31	7,69	12,31	26,15	20	15,38	6,15	4.05
Insurance companies	12,31	9,23	10,77	26,15	20	20	1,54	3.98

Table 22: When you see the information DataBait reveals about you, how much would you worry if X has access to this information? (1 = very concerned, 7 = very unconcerned) (%, iMinds n=65)

LTU

	Very concerned	Somewhat concerned	Neutral	Somewhat unconcerned	Very unconcerned	Weighted Average
Your friends on Facebook	2,5	17,5	22,5	12,5	45	2,2
Facebook	17,5	20	32,5	15	15	3,1
Other Facebook companies	15	42,5	15	20	7,5	3,38
State security	5	17,5	35	22,5	20	2,65
Advertisers	25	32,5	17,5	10	15	3,42
Insurance companies	12,5	32,5	22,5	12,5	20	3,05

Table 23: When you see the information DataBait reveals about you, how much would you worry if X has access to this information? (1 = very concerned, 5 = very unconcerned) (%, LTU n=40)

Conversely, respondents were most divided with regard to advertiser and insurance companies. Figure 12 shows that respondents are most concerned if they share too much with their friends, followed by State security, Facebook and on equal measure other Facebook companies, advertisers and insurance companies. What is more, the whole population is most unanimous with regard to friends on Facebook and state security. This is so because there are no equal amounts of unconcerned respondents and very little neutral entries. Conversely, respondents were most divided with regard to advertisers and insurance companies.

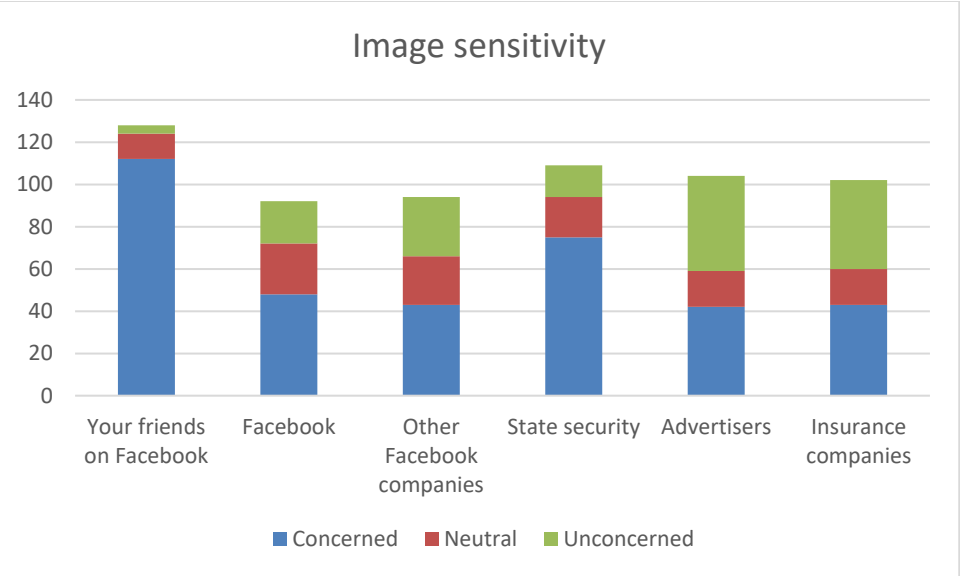

Figure 12: Image sensitivity (iMinds n=65, LTU n=40)

3.5 Disclosure scoring framework

The disclosure scoring framework was rather easy to use, as indicated by the mean scores for both living labs (5,49 for iMinds and 4,97 for LTU) in Table 24. What is more, this feature was not difficult to locate as respondents found it rather easy to locate on average (Table 25). So we can conclude that this feature works fine in terms of usability.

Since quite a long text popped up upon visiting this component, it was interesting to see how well users understood these concepts. In this regard, both living lab participants agreed that the text was rather easy to read (Table 26).

How easy or difficult was this task?	iMinds	LTU
Very difficult	2,13	3,13
Difficult	2,13	6,25
Rather difficult	6,38	9,38
Neutral	6,38	28,13
Rather easy	17,02	9,38
Easy	38,3	12,50
Very easy	25,53	32,25
Mean score	5,49	4,97
	n=47	n=32

Table 24: Disclosure scoring framework usability (%)

How easy was it to find this function?	iMinds	LTU
Very difficult	4,26	3,13
Difficult	2,13	3,13
Rather difficult	2,13	12,50
Neutral	6,38	9,38
Rather easy	10,64	21,88
Easy	44,68	6,25
Very easy	29,79	43,75
Mean score	5,7	5,38
	n=47	n=32

Table 25: Disclosure scoring framework usability (%)

How difficult was it for you to understand the language and concepts (words) used in this page?	iMinds	LTU
Very difficult	4,26	0
Difficult	2,13	0
Rather difficult	8,51	15,63
Neutral	14,89	15,63
Rather easy	31,91	15,63
Easy	23,4	21,88
Very easy	14,89	31,25
Mean score	4,98	5,38
	n=47	n=32

Table 26: Disclosure scoring framework usability (%)

Participants were also asked for each disclosure category (dimension), if they were surprised by the produced results; i.e. if they thought they were not disclosing it but DataBait shows that they actually do. Interestingly, the average over all dimensions for iMinds was 4,17 and 4,3 for LTU (Table 26), leading to the result that in many cases DataBait manages to unveil information that the users thought were not visible. This result also indicates the efficacy of the developed inference mechanisms. In Figure 13 the following categories were considered the most surprising : Health, psychology, political views and religion.

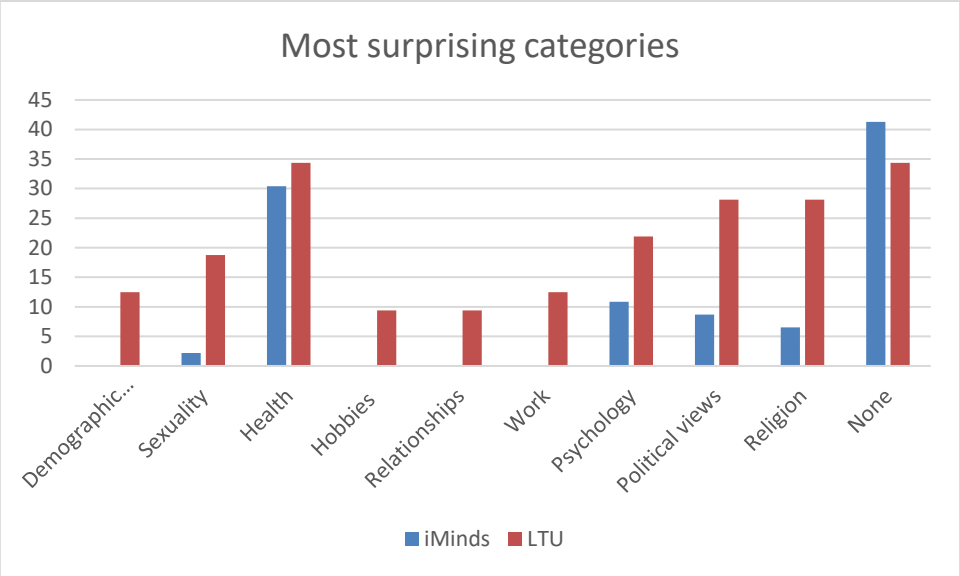

Figure 13: Disclosure scoring framework most surprising categories (%, iMinds n=47, LTU n=32)

What category surprised you the most?	LTU
Demographic information	4,72
Sexuality	4,44
Health	4,13
Hobbies	4,69
Relationships	3,81
Work	4,22
Psychology	4,22
Political views	4,31
Religion	4,16
	n=32

Table 27: Disclosure scoring framework usefulness (%)

Is this feature a good summary of your disclosed habits and/or personality?	IMINDS	LTU
Yes	46,81	75,00
No	53,19	25,00
	n=47	n=32

Table 28: Disclosure scoring framework usefulness (%, iMinds n=47, LTU n=32)

Is this feature useful to identify potentially sensitive information?	IMINDS	LTU
Yes	68,09	100
No	31,91	0
	n=47	n=32

Table 29: Disclosure scoring framework usefulness (%, iMinds n=47, LTU n=32)

Looking at the usefulness of the tool as a summary of users' digital footprint, respondents were very convinced in LTU's case, 75% of participants agreed that disclosure scoring framework provided a good summary of their disclosed habits and personality. In iMinds' case, only a smaller half of participants agreed (46,8%). In total, around 60% of the users thought that the disclosure scoring framework provided a good summary of their habits and personality. This can be considered as quite satisfactory, considering also the fact that a large number and wide range of user attributes are considered, meaning that many predictions are produced for each user and this increases the possibility of producing inaccurate predictions for at least some attributes.

To what extent do you think the liked pages and posts are related to your most sensitive privacy category?	iMinds	LTU
Totally unrelated	13,64	9,68
Unrelated	23,865	6,45
Neutral	42,045	19,35
Related	20,455	22,58
Totally related	0	12,90
N/A	0	29,03
Mean score	2,66	3,32

Table 30: Disclosure scoring framework: relativity of pages and posts (%, iMinds n=47, LTU n=31)

Respondents were also asked about the control assistance tool that provides to the user lists of pieces of content with high contribution to the disclosure score, prompting him or her to reconsider sharing that content. Most participants were neutral to the question if the shown content is related to their most sensitive category (Table 30). Nevertheless, the Belgian participants tended to think they were rather less related, while the Swedish partipants tended to think they were rather more related.

Also, as indicated by the results in Table 29, both labs support the goal of this tool: they both think that the disclosure scoring framework is a good tool to identify potentially sensitive information. More particularly 68,1% of iMinds' participants and all LTU's participants agree that these tools are useful for identifying potentially sensitive content.

How easy or difficult was it to change your disclosure scoring sensitivity?	iMinds	LTU
Very difficult	6,67	6,45
Difficult	6,67	9,68
Rather difficult	8,89	3,23
Neutral	13,33	22,58
Rather easy	15,56	6,45
Easy	40	19,35

Very easy	13,33	32,26
Mean score	5,02	5,00

Table 31: Disclosure scoring framework changing sensitivity (%, iMinds n=47, LTU n=31)

How easy or difficult was it to locate this function?	iMinds	LTU
Very difficult	6,67	9,68
Difficult	6,67	0
Rather difficult	2,22	6,45
Neutral	13,33	19,35
Rather easy	15,56	12,90
Easy	40	25,81
Very easy	15,56	25,81
Mean score	5,07	5,06

Table 32: Disclosure scoring framework: changing sensitivity usability (%, iMinds n=45, LTU n=31)

How certain are you that you fulfilled this task successfully?	iMinds	LTU
Very uncertain	6,67	25,81
Uncertain	6,67	0
Rather uncertain	4,44	6,45
Neutral	13,33	6,45
Rather certain	22,22	16,13
Certain	33,33	6,45
Very certain	13,33	38,71
Mean score	5,84	4,61

Table 33: Disclosure scoring framework: changing sensitivity usability (%, iMinds n=45, LTU n=31)

In the last part of the micro task, users were asked to change the sensitivity of their disclosure dimensions. Users found this rather easy to do, could find this function easily and lastly, most respondents were rather certain that they fulfilled this task successfully.

As shown in Table 34, a majority of both living labs did consider to delete a post or dislike a page. In the interviews we learned that all respondents already curate their online identity, which means that they have less to no content to delete. However, they did find it useful to have filters to look for particular kinds of data (Table 35).

Based on the information provided, have you considered to dislike a page or delete your post?	iMinds	LTU
Yes	32,56	45,16
No	67,44	54,84

Table 34: Controlling disclosure (%, iMinds n=44, LTU n=31)

Did you find the per category filters useful?	LTU

Yes	58,06
No	41,94

Table 35: Controlling disclosure usefulness (%, LTU n=31)

Lastly, respondents indicated how concerned they would be if one of the following parties had access to their disclosure scoring framework results.

	Very concerned		Concerned		Neutral		Unconcerned		Very unconcerned		Mean	
	iMinds	LTU	iMinds	LTU	iMinds	LTU	iMinds	LTU	iMinds	LTU	iMinds	LTU
Your friends on Facebook	31,91	59,38	51,06	21,88	12,77	12,5	4,26	3,13	0	3,13	1,89	1,69
Facebook	12,77	31,25	36,17	21,88	27,66	18,75	21,28	12,5	2,13	15,63	2,64	2,59
Other Facebook companies	12,77	31,25	25,53	9,38	27,66	21,88	27,66	21,88	6,38	15,63	2,89	2,81
State security	21,28	46,88	31,91	18,75	31,91	21,88	8,51	3,13	6,38	9,38	2,47	2,09
Advertisers	12,77	15,63	21,28	21,88	34,04	31,25	23,4	9,38	8,51	21,88	2,94	3
Insurance companies	12,77	31,25	19,15	21,88	36,17	21,88	23,4	12,5	8,51	12,5	2,96	2,53

Table 36: When you see the types of information that could be retrieved from your profile, how much did you worry about who sees this information? (Likert scale 1= Not worried at all, 5=Very Worried) (%, iMinds n=44, LTU n=32)

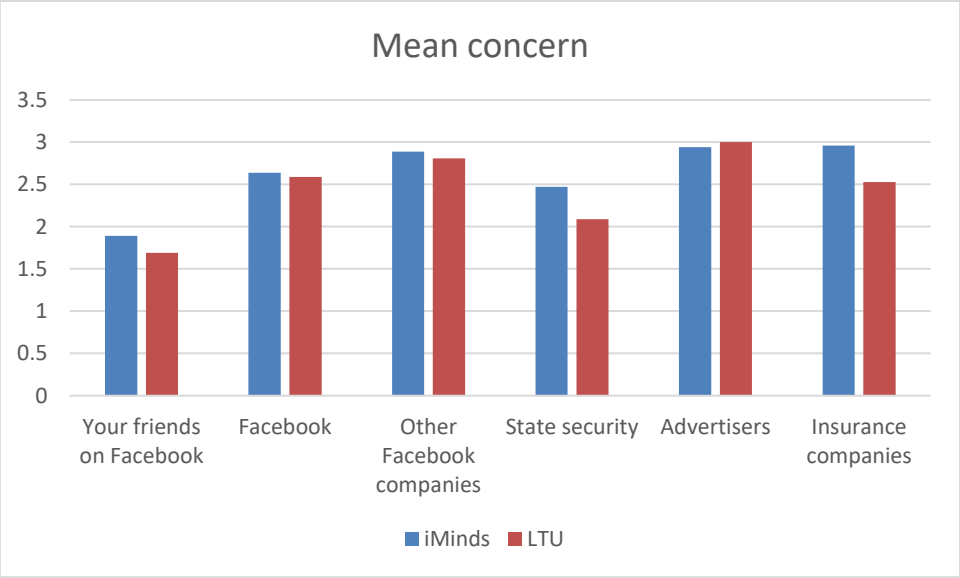

Figure 14: Level of concerns per party accessing sensitive information (scale 1= Not worried at all, 5=Very Worried)

With regard to the information the disclosure scoring framework could derive from respondents' data, we can see that our users are more concerned when this data falls into hands of third parties such as insurance companies, advertisers and other Facebook companies. These results are opposite to those of image leaks. Here respondents were more worried about what they disclosed to their friends.

3.6 Drop-out survey

Due to technical issues related to Facebook API limitations, the second pilot was affected by server heavy load and this reduced the functionality of the DataBait tool. For this reason, we experienced user drop-out, especially in the Swedish study, because it was started earlier. We have investigated the reasons of drop-out and found out DataBait related and non-related issues. The drop-out survey was designed after completion of the pilot and sent out to the people who showed interest but did not complete the tasks completely. The survey can be found in Annex 5. The importance of conducting this study was to find the issues in the DataBait application in order to improve future developments.

In the Swedish pilot, a total of 118 users showed their interest and completely filled out the intake survey. However, 53 participants completed more than one microtask (i.e. got involved in the DataBait application test) but only 27 of them filled out all five microtasks. Accordingly, due to relatively high drop-out rate, a qualitative survey was conducted to understand why users drop-out of this user study before the deadline and completing the assigned tasks. The drop-out survey was sent to all 91 users who filled out the intake survey but did not complete the test. In sum, we received 32 complete responses. Of these, 14 responses were from those who had been involved in the DataBait test and completed two or more microtasks (referred as dropped-out users). The other 18 responses were from the users who filled out the intake survey but did not participate in the DataBait application test or dropped-out after the first microtask (referred as non-participants).

Regarding the dropped-out users, in response to an open-ended question about their drop-out reason, instability or non-functionality of the prototype was the most influential factor that has been mentioned by six test-users. They encountered many problems while trying to log in to

the DataBait application. Some users also complained that the microtasks were hard to understand, too long, exhausting and the instructions on how to do the tasks were not clear enough. Inflexibility of the DataBait application due to incompatibility with the smartphone was the next affective factor on their drop-out decision. Limitation of access to a computer or internet, insufficient reminders and too close in time microtasks with too strict deadlines were other influential factors on their motivation. Bad timing of the test (due to summer holiday) and limitation of their time were also other de-motivational factors.

When it comes to non-participants, privacy concerns due to personal questions and insecurity about the DataBait application were mentioned by seven users. Similar to dropped-out users, complexity of the microtasks besides the lack of an easy to access and clear instruction were also very influential on their motivation. The forgetfulness of the users and their request to receive more than one reminder was another important factor. Summer holiday and time intensity of the tasks were the next discouraging factors. Some users also were dissatisfied due to incompatibility with the smartphone or non-functionality of the DataBait application when they tried to login to the application.

The results of our survey confirm that the motivations and expectations of the participants will change over the time and it is difficult to get the same level of motivation during the period of their involvement. In this way, the performance of the prototype plays a significant role on keeping users motivated. More specifically, when the users have access to all tasks and they can complete the tasks at their own paces, they usually are willing to complete the tasks altogether. In this case, upon encountering technical problems, they decide to not devote more time and effort to participate in the activity. Therefore, it is of importance to manage users' expectation throughout the whole period of the user study by making clear to users that the prototypes may not work as commercial or final version.

The next notable point is the importance of reminders. Although in this test, all users received at least one reminder for each microtasks, many of them did not complete the test due to forgetfulness and they expected to receive more than one reminder. It could be better if they are asked about the number of reminders that they expect to receive. Another lesson learnt from the survey results is that, the task should be designed as easy to use and easy to understand as possible. If it is not possible to simplify the task though, it should be divided to sub-tasks.

3.7 Feedback survey

In the section below, we shortly discuss the results of the feedback survey. These are divided in a section with regard to the usability of the whole system and a second part that focuses on the most important features of DataBait.
In Table 37 an overview is presented of the general system usability level. Here we can see that the average ratings are around the mid value of 2,5, so the system in general is acceptable, but not more. More work has to be done with regard to reducing the complexity of the product, by explaining how it should be used and reducing inconsistency. However, keeping the results of the drop-out survey in mind and the general technical issues experienced during the pilot, we can expect that this influenced the general usability of the DataBait application greatly. This means that if we did not experience Facebook’s API changes, then a much better usability score would be given. This is so because respondents evaluated the new features more positively than before despite these challenges.

	Strongly disagree		Disagree		Neutral		Agree		Strongly agree		Rating average	
	iMinds	LTU	iMinds	LTU	iMinds	LTU	iMinds	LTU	iMinds	LTU	iMinds	LTU
I think that I would like to use this product frequently,	16,67	21,43	36,11	21,43	13,89	39,29	33,33	14,29	0	3,57	2,64	2,57
I found the product unnecessarily complex,	22,22	25,00	41,67	32,14	16,67	28,57	13,89	14,29	5,56	0,00	2,39	2,32
I thought the product was easy to use,	5,56	10,71	11,11	14,29	11,11	28,57	55,56	32,14	16,67	14,29	3,67	3,25
I think that I would need the support of a technical person to be able to use this product,	44,44	53,57	38,89	10,71	8,33	25,00	5,56	7,14	2,78	3,57	1,83	1,96
I found the various functions in the product were well integrated,	5,56	3,57	19,44	10,71	38,89	35,71	36,11	39,29	0	10,71	3,06	3,43
I thought there was too much inconsistency in this product,	2,78	17,86	55,56	28,57	19,44	42,86	13,89	10,71	8,33	0,00	2,69	2,46
I imagine that most people would learn to use this product very quickly,	2,78	14,29	13,89	17,86	25	25,00	44,44	35,71	13,89	7,14	3,53	3,04
I found the product very awkward to use,	13,89	21,43	47,22	32,14	13,89	17,86	16,67	17,86	8,33	10,71	2,58	2,64
I felt very confident using the product,	2,78	14,29	25	17,86	38,89	25,00	30,56	35,71	2,78	7,14	3,06	3,04
I needed to learn a lot of things before I could get going with this product,	27,78	42,86	47,22	25,00	8,33	21,43	13,89	3,57	2,78	7,14	2,17	2,07

Table 37 System Usability Scale (%, iMinds n=36, LTU n=28)

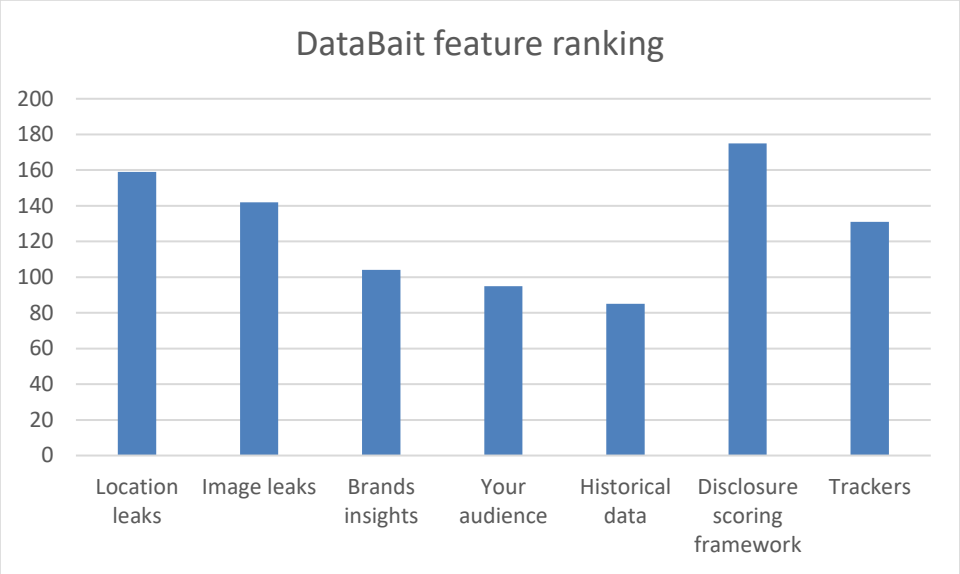

Figure 15 DataBait feature ranking (iMinds n= 36)

Respondents were able to rank DataBait features in order of importance. By assigning values to each rank (1st place = 7, 7thplace = 1), a total score is assigned per component. As shown in Figure 15, Your disclosure scoring is most important followed by Location and Image leaks. Despite not being evaluated in this pilot[3], trackers were ranked next, so it is important to note that participants were higly interested in this feature despite its absence.

3.8 Extra information feedback

iMinds investigated the relevance and perception of additional information in DataBait via the provision of a summarised DLA, the already present information and new information added within the pilot survey. We first report on the DLAs, then the additional information provided within the survey and next we use the qualitative results to further frame the relevance of different kinds and forms of extra information.

3.8.1 DLA comparison

Both living labs reported similar outcomes for both types of DLAs with regard to usability and retention of information. It was to be expected that the total reading time of the longer DLA would be longer and this was the case. So based on the quantitative information, there is no reason to have a summary of the DLA. But based on the qualitative feedback where users could compare both versions, all respondents were unanimously more positive about the summarised DLA. This is so because it invited them to read (although most respondents read both DLA because these were part of the survey and they saw this as part of the exercise). Regardless of users readership all interviewees want a summary with links to the full DLA in case something needs to be read more closely. As such, we can conclude that a summarised DLA lowers the threshold to read, but it does not necessarily change retention if the DLA is read.

[3]A Chrome update a few days before the pilot disabled this feature.

3.8.2 Information form comparison

In this pilot, respondents were exposed to multiple kinds of placement of additional information[4] : pop-ups, information on the left-hand side of visualisations, in the living lab surveys, the DLA and a FAQ. Next, the information itself could be presented as text with paragraphs, text with paragraphs and titles and lastly text with paragraphs, titles and bullets.
Next to this form factor, the information was also varied in types of information : this could refer to how a feature works, what the results mean, how to use a feature and lastly what can be done as a next step. In the case of information shown on the side, and the pop-up, the information provided referred to the technological process that took place: how things work. In the surveys we provided additional information in case users wished to change something based on the output DataBait provided.

Placement
What form of information is best depends on the need for information in a given situation. For example, if a DataBait visualisation is self-explanatory like Image leaks, Location leaks, Your audience, then users do not require any messages that disrupt their experience. If a visualisation requires user actions or if this visualisation is rather complex, then our respondents require a message that explains what they can do, how they can do it and what the visualisation means. This was the case for Your disclosure scoring (here a pop-up was shown). For the latter, users were not annoyed by the pop-up they received to inform them about Your disclosure scoring, this was seen as relevant information. All male interview participants did report that they clicked away the pop-up before reading it and only in hindsight understood how relevant this information was. In this regard, DataBait would be better if the question mark to recall the pop-up would be more visible than it is now.

What happened here is, that these men could only see that they required extra information after experiencing a lack thereof. When asked how they usually gather information on websites, they said they are exploring and finding out how things work while they are using them. For this type of user, extra information should be embedded in question marks that are easy to find and relevant.

Rita reported that she really liked the step by step approach in the survey. This step by step explanation of how to use tools aided her to see how and what each tool did. She said she would be interested in having a tutorial for each feature. This is highly recommendable since future users will not be partaking in the survey and will receive less instructions as a consequence.

Form
Users prefer, paragraphs, with titles and bullets because the text looks easier digestible than large blocks of texts (referred to as typical terms of service by interviewees). This result is not surprising and Suzy said that the more a text is divided in subtitles and bullets, the more easily she can scan it without actually having to read each part to find information relevant to her situation.

[4]Note that LTU received all forms except for additional information in the survey. They are not considered here because they were not interviewed afterwards.

Types of information
Participants were the least interested in how things work. This information was not required for the pilot exercise or to better understand the visualisation. The latter is also possible because the visualisations are quite straightforward. Information that told users how to use a feature was more interesting, but only after users experienced a need for it. More careful users will experience this from the start, while exploring users only experience this when something does not make sense.
Lastly, there was little interest with regard to next steps. Given the information users received, almost no interviewees were interested in how to change or delete Facebook content because they already knew how, but more importantly because there was no need to do so. So in this case, the information was not relevant.

General remark
Information relevance depends on the experienced need for information. This was also the case for the visualisations and other output of DataBait we provided to our respondents.
In two cases, Image leaks or Your disclosure scoring, DataBait provided a prediction with regard to sensitivity of content. In these cases, the relevance of the predictions depended on the fact that respondents felt they had something to hide or not. Our two female interviewees had their reasons to hide either medical information or political views. As a result, they understood the relevance of our tools to screen their UGC for this type of sensitive information. The male respondents of the interviews had nothing to hide because they did not think any of their content could cause issues in the near future.

During these interviews, we felt that the relevance of predictions with regard to sensitivity of information depend on particular situations people may be in at that time of their lives. But this is a very idiosyncratic way of reviewing digital footprints. It depends on users' knowledge of threats and possible future scenarios. As a result, we asked each interviewee if they would find our predictions more relevant if we could tie them to particular threatening scenarios: what information is required for identity theft, future employers, etc. The answer was positive, respondents explained that they lacked the knowledge or imagination to review their footprint from this angle. So, adding these scenarios would enhance the relevance of all DataBait's predictions.

3.9 General recommendations

Improve stability as an ongoing effort
Despite the unstability of the system, our respondents were still positive about DataBait as a tool to increase their awareness. If there were no technical issues, their opinion would have been even more positive, so this is a challenge that requires an on-going effort. The technical problems of the system were discussed with the USEMP consortium and the respective partners have already addressed them.

Add tutorials
The pilots have been tutorials where surveys explained how to use DataBait step by step. In order for future users to understand all the functions of our tool, a tutorial is required. This was discussed within the project and seminars/tutorials are included as part of the exploitation path for the USEMP project.

Improve the relevance of provided information

The quality of the information provided by DataBait as output should be increased further through technical innovation and qualitative research. In D6.5 additional information will be added to trackers. This information refers to the contents of visited websites: if a website is about football, trackers may deduce that you are interested in football. Secondly, we should further improve DataBait by identifying relevant scenarios or threats so that users can review their digital footprint in different possible future scenarios. One of the best means to identify these scenarios and evaluate their relevance is through qualitative research. All these future enhancements of the DataBait are being taken into account for the evolution of the project after the end of the USEMP project.

Different information needs

The quality of DataBait as a tool for awareness can only increase if DataBait can be developed to account for the different information needs required by different types of users in different situations on DataBait. This means that where possible, we have to summarise information with in subtitles, bullet points and visuals so that users can see at a glance what information is relevant to them. Since not everyone will have the same needs, we need a layered approach where more information is given if it is required.

Lastly, the additional information we offer now should be made more accessible, the majority of the interviewees told me they could not find the pop-up of Your disclosure framework and none of them knew there was a FAQ with additional information, something that is already improved in the current version of DataBait.

4 Conclusion

We have reported on the pilots aimed to let end-users evaluate DataBait. While there were minor technical challenges during the pilot, we can say two things. First, enough respondents were able to provide feedback and second, the feedback is positive, despite technical hickups that decreased stability.

When we couple this back to our iterative design approach, which entails an interaction between end-user and developer, we can say that we were successful in addressing user needs through technology and user participation. This is so because participatory workshops enabled USEMP as a whole to identify needs. These needs have been translated to requirements for DataBait's design. Lastly, the design was user-tested again to see if our identified needs were addressed properly.

5 Bibliography

Dinev, T., & Hart, P. (2004). Internet Privacy, Social Awareness, And Internet Technical Literacy–An Exploratory Investigation. *BLED 2004 Proceedings*, 24.

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. https://doi.org/10.1007/s12394-009-0019-1

Popescu, A., Hildebrandt, M., Breuer, J., Claeys, L., Papadopoulos, S., Petkos, G., … Padyab, A. (2016). Increasing Transparency and Privacy for Online Social Network Users – USEMP Value Model, Scoring Framework and Legal. In B. Berendt, T. Engel, D. Ikonomou, D. Le Métayer, & S. Schiffner (Eds.), *Privacy Technologies and Policy* (Vol. 9484, pp. 38–59). Cham: Springer International Publishing.

Rainie, L. (2015, December 30). Americans conflicted about sharing personal information with companies. Retrieved from http://www.pewresearch.org/fact-tank/2015/12/30/americans-conflicted-about-sharing-personal-information-with-companies/

Topline: Sharing personal information with companies. (2015, December 29). Retrieved from http://www.pewinternet.org/2015/12/29/americans-conflicted-sharing-personal-information-topline/

6 Annexes

6.1 Annex 1: living lab invitation

"Dear…,

Do you ever wonder what happens with your Facebook or browsing data? And more importantly what other parties may deduce from your data? We are in the process of creating a tool to help those who want to know more about how their data is used by Facebook and third parties.

Within USEMP, we try to create a tool to help you understand what happens with your data and help you on your way to change or delete parts of your personal information if you feel they should not pass through the hands of third parties.

If you would like to participate, in making sure this tool provides you and other users with relevant information and features, please participate. Your feedback and suggestions will be implemented during the course of this living lab. What is more, you will learn about your own online privacy and means to change aspects you no longer like.

We will ask you to perform tasks such as filling in short surveys, use our tool and report on what you did with the tool. Next we will conclude this project with an interview at a location of your choice that will last for one hour. The period that we need your input runs from the beginning of February to the 3th week of February.

Best regards,"

6.2 Annex 2: Detailed living lab tasks

6.2.1 Initial measurement and Micro task 1: registration

Registering with DATABAIT

Get respondents to log in on DATABAIT (This requires an admin to add their user ID to the DB app in Facebook[5])

Ask about the usability of the process, their attitude towards sharing this information with DATABAIT and lastly, when they actively thought about disclosing information.

Install the DATABAIT plugin in Firefox or Chrome

Respondent instructions

Welcome to your first assignment. During this assignment we will ask you to do three things for us. Fill in a short survey, register and install a plug-in.

Visit the survey here and fill in the questions until you are told otherwise.

Next, visit https://databait.hwcomms.com and register by reading the instructions on this website. Also, open this survey and fill in the questions after completing this process. In case you encounter problems, you can mail them or add them in the survey at the remarks section.

[5] https://developers.facebook.com/apps/1547194038870780/dashboard/.
https://developers.facebook.com/apps/1547194038870780/dashboard/.

Remember that the DATABAIT tool only works with Chrome and Firefox.

After completing the registration process, please fill in the following questionnaire:

1. How easy or difficult was this task? (1 = very hard, 7 = very easy)
2. How confident are you that you fulfilled this task successfully? (1 = I am not confident at all, 7 = I am very confident)

If you experienced issues during the registration process you can describe them here. Feel free to suggest how we could solve this issue in the future.

First at any point express how much you agree or disagree with the following statements: During the registration process have you felt …

1. Discouraged with the amount of effort needed to understand what would be done with your data?
2. Confused by the information provided in the Data Licence Agreement?
3. Confident that you understood what would be done with your data?
4. Impatient because you wanted to learn more but needed to make a decision right away?

Open question:

Could you please elaborate when you considered whether or not to share information about yourself during the registration process? What did you decide and why?

6.2.2 My dislosures and Photo insights

Please go to the DataBait app, click on "My Disclosures" and go to Photo Insights. Next use this function to see what your Facebook pictures reveal about you. Try to stay on this page and see what could be found on this page. After that fill out this questionnaire:

1. How easy or difficult was this task? (1 = very hard, 7 = very easy)
2. How confident are you that you fulfilled this task successfully? (1 = I am not confident at all, 7 = I am very confident)
3. How easy was it to find this function? (1 = very hard, 7 = very easy)
4. How difficult was for you to understand the language and concepts (words) used in the image leaks? (1 = very hard, 7 = very easy)
5. In general, how accurate are the information provided for your whole image collection? (1 =not accurate at all, 7 = very accurate)
6. In general, how accurate are the information provided for a single image? (1 =not accurate at all, 7 = very accurate, Uncertain)

If you encountered any problems or found points we can improve, please let us know below: First at any point express how much you agree or disagree with the following statements: During the registration process have you felt … (7 point likert: 1: I completely agree – 7: completely disagree)

1. Discouraged with the amount of effort needed to understand what was done with your data
2. Confused by the information provided by image leaks

3. Confident that you understood what was done with your data
4. Impatient because you wanted to learn more but needed to make a decision right away
5. Discouraged with the amount of effort needed to understand how to change this information

Open question:

- Could you please elaborate when you considered whether or not to change information about yourself shown in the Photo Insights tool. What did you decide and why?

6.2.3 Location leaks

1. Analogous to image leaks
2. Brand detection in images
3. Analogous to image leaks

After the micro task

After each micro task, we will summarise the feedback provided by all respondents in order to highlight what parts of DATABAIT require improvements. We will invite respondents to suggest improvements on the blog by the time of the next micro task or from as soon as they see the summary.

Please tell us if you have, from the first questionnaire until so far, experienced any issue or would like to give any suggestion that could help us:

6.2.4 Micro task 3: Friends influencer and 3rd party tracking

These are analogous to the example provided in image leaks

Audience Influence

From DataBait's main screen click on Audience Influence and wait for sometime for the result to load. Read the information about the page on the left side and answer the following questions:

Detailed Interactions

Within the Audience Influence page click on the next tab "Detailed Interactions". Read the information on the left side of the page. Try to click on different circles and see what happens. Try to play around with the bubbles and then answer the following questions:

[same as image leaks]

Statistical Data

Under Audience Influence page click on Statistical Data. Look at the information provided and then answer the following:

[same as image leaks]

User Trackers

From the main DataBait screen click on Trackers icon.

visit cnn.com

o open any news item

o on the right side there a share to social media option

o open DataBait plugin

- list all trackers
- find “gigya tracker” (share in social media) and disable it
- re-load page (automatically)
- social media share option is not shown

6.2.5 Feedback survey

Here we will ask questions similar to the initial measurement survey to be able to measure an increase in awareness. In case we lack the time to roll out these surveys, the feedback survey will be part of the F2F interviews (see below).

6.3 Annex 3: Intake survey

- Do you have a Facebook account? (If not, end the survey)

Internet access and browser

- Do you have access to internet at home? (If not, end of survey)
- Can you use one of the following browsers for a month? (If something else, end of survey)
  - Chrome
  - Firefox

Facebook usage

How often do you use Facebook?

- Never
- Very sparsely
- Monthly
- Weekly
- Daily
- Multiple times a day

Socio-demographic

What is your gender?

- Male
- Female
- Other

What is your birth year?

What is your education level?

Can you provide us with your Facebook ID?[6]

6.4 Annex 4: Interviewed respondents

Pseudonym	Age	Date of interview	interviewer

[6]The latter is required to register users to DataBait on Facebook because this applicaiton is still in development.

Max	26	02-Mar-16	Rob
Hanne	29	08-Mar-16	Rob
Bart	38	08-Mar-16	Rob
Tom	46	07-Mar-16	Rob
Matilda	24	17-Mar-16	Paulien
Peter	28	17-Mar-16	Paulien
Donna	26	15-Mar-16	Paulien
Marc	22	15-Mar-16	Paulien
Eric	26	29-Feb-16	Ali
Stan	22	1-March-16	Ali
Kenny	27	4-March-16	Ali
Kyle	26	4-March-16	Marita

6.5 Annex 5: Drop out survey

How to Sustain User Engagement?

Thank you for your participation, your answers are valuable feedback to our research.

Some weeks ago you showed us your interest for participation in our research project by providing us with your email address and Facebook URL, but unfortunately you did not complete the tasks. In this questionnaire we are interested in knowing why people drop-out of user studies before projects or activities have ended. The data collected by this questionnaire will be used strictly and exclusively for the purposes of research on how to sustain user engagement over time. This information will never be shared, sold or used for any other purpose.
The questionnaire consists of 22 questions and will take you approximately 20 minutes to complete. If you have

any questions about the survey please contact: Abdolrasoul.Habibipour@ltu.se.

Backgroundquestions

1. Gender

- ◯ Female
- ◯ Male
- ◯ Other

2. Age

- ◯ 17 oryounger
- ◯ 18-25
- ◯ 26-35
- ◯ 36-45
- ◯ 46-55
- ◯ 56 orolder

3. Level of Highest Educational Attainment:

- ◯ Did Not Complete HighSchool
- ◯ HighSchool
- ◯ Some College
- ◯ Bachelor'sDegree
- ◯ Master'sDegree
- ◯ Advanced Graduate work orPh.D.
- ◯ Other (pleasespecify)

4. What is/was your...

Field ofstudy	
Professionalskills	
Workexperiences	

Descriptive questions

We saw that you participated in the DataBait-application development, but did not follow complete the task.

5. Please clarify your situation regarding to the ***previous*** phase(s) of DataBait test which was held in March 2016.

- ◯ I did not participate in thattest.
- ◯ IparticipatedinMarch2016test,andcompletedtheassignedtask(s).
- ◯ IparticipatedinMarch2016test,butIdidnotcompletetheassignedtask(s).

* 6. What were your initial motivations when you signed up in the DataBait application development?*[Please prioritize your answers from most important motivator to least important motivator]*

* The mostimportant	
The secondimportant	
The thirdimportant	
The leastimportant	

* 7. What were your main reasons for dropping out of the DataBait application development?*[Please go into as much details as possible and prioritize your answers from most important reason to least important reason]*

* The mostimportant reason	
Secondreason	
Thirdreason	
Fourthreason	
The least importantreason	

8. Whatcouldwe,asorganizersoftheDataBaittest,improveinordertore-engageyouasaparticipant?

9. If these changes are met, would you return to the user study?

Yes

No,I'llnotreturntotheprojectanymore(pleasespecifywhynot)

10. Do you think you will participate in other similar user studies in the future?

Yes

No

I'm notsure

Performance of the prototype

* 11. Please indicate how influential each of the following factors were in your decision to drop-out.

I felt discouraged and/or disengaged because...

	Not influential at all	A little influential	Somewhat influential	Very influential	Extremely influential
the prototype was not easy to use	○	○	○	○	○
the prototype was not easy to understand	○	○	○	○	○
the prototype was not reliable	○	○	○	○	○
the prototype was not stable and mature	○	○	○	○	○
the prototype was not easily accessible	○	○	○	○	○
the novelty aspects of DataBait application quickly disappeared	○	○	○	○	○
the prototype did not meet my expectations	○	○	○	○	○

* 12. Did you encounter any software bugs or errors that made you unable to continue using the prototype?

○ No

○ Yes

In which phase or step of using the prototype (e.g., installation, use of prototype, etc.) you faced these problems and how? Please write as much details as possible.

Other related technical aspects

* 13. Please indicate how influential each of the following factors were in your decision to drop-out.

I felt discouraged and/or disengaged because...

	Not influential at all	A little influential	Somewhat influential	Very influential	Extremely influential
I had not been informed about the project's details before start participation	○	○	○	○	○
I was not satisfied with the technical support during my involvement period	○	○	○	○	○
there was no clear guideline on how to do the tasks	○	○	○	○	○
I had not been trained sufficiently to participate	○	○	○	○	○
I encountered technical constraint of my devices such as RAM or Hard disk drive	○	○	○	○	○
I had to consume my own private resource such as battery and computation power of my device	○	○	○	○	○
I had to consume my own internet data quota	○	○	○	○	○
I had concerns about my privacy	○	○	○	○	○
I had concerns about the security of my information	○	○	○	○	○

* 14. Were you satisfied with the preparations, training and clear guidelines before and/or during the project?

- ( ) Not Applicable
- ( ) Yes
- ( ) No

Please specify why not

* 15. Were you satisfied with the technical support?

- ( ) Not Applicable
- ( ) Yes
- ( ) No

Would you give us an example.

Social aspects

* 16. Please indicate how influential each of the following factors were in your decision to drop-out.

I felt discouraged and/or disengaged because...

	Not influential at all	A little influential	Somewhat influential	Very influential	Extremely influential
the received financial reward was smaller than expected	○	○	○	○	○
I had not enough time to be involved in this project	○	○	○	○	○
I was not able to participate in this project at my own pace	○	○	○	○	○
the tasks' deadlines for each step were strict and inflexible	○	○	○	○	○
there was a long gap between the project's steps	○	○	○	○	○
it was a lengthy project	○	○	○	○	○
timing of the project was inappropriate	○	○	○	○	○

17. Please let us know if you encountered any problems with the gaps between project's phases, longevity of the project or timing of the activity.

Relationship with the developers

* 18. Please indicate how influential each of the following factors were in your decision to drop-out.

I felt discouraged and/or disengaged because...

	Not influential at all	A little influential	Somewhat influential	Very influential	Extremely influential
the point of contact was unclear/variable and there was no fixed contact person	○	○	○	○	○
there was no mutual trust with the developers	○	○	○	○	○
the project developers did not give me this feeling that my contribution is important	○	○	○	○	○
I was not informed about the project's results	○	○	○	○	○
my feedback was ignored by the developers	○	○	○	○	○
I was not satisfied with the way(s) in which I received feedback from the project	○	○	○	○	○
I was not satisfied with the way(s) in which I sent my feedback to the project	○	○	○	○	○

* 19. Specify the way(s) you and the developers stayed in contact during the project:

- [ ] In person
- [ ] E-mail
- [ ] Phone
- [ ] Text message (SMS)
- [ ] Fax or mail
- [ ] Social media network
- [ ] Skype
- [ ] Other (please specify)

20. Please let us know if you encountered any problems while interacting with the developer's team.*[Or if your feedback was ignored by the developers.]*

21. Is there something else, not covered by this survey, you think is relevant for your decision to drop-out?

* 22. Email address:

We need your email address to be able to send your gift.

Thank you

Thank you so much for your participation in our survey. We will shortly after receiving your feedback send the survey reward to your email address. If you haven't received it one month after completing the survey, please contact Abdolrasoul.Habibipour@ltu.se.

6.6 Annex 6: CERTH survey

The following close-ended questions were asked :

1. What is your gender ?
2. What is your nationality ?

3. What is your highest educational degree ?
4. What is your working situation ?
5. What is your relation status ?
6. What is your living situation ?
7. What is your religion ?
8. Do you practice this religion ?
9. What is your sexual preference ?
10. What is your political preference ?
11. What is your health status ?
12. Pick corresponding brand preferences and general interests , such as music, sports, etc.

Open ended questions :

13. What is your length ?
14. What is your weight ?

6.7 Annex 7: DLAs

6.7.1 Version A, the short DLA

Below we list some important points from the contract (the 'data licensing agreement' or DLA) that you have to sign before you can use DataBait. This list cannot replace the contract. It is merely a summary, so please make sure you have read the complete contract and if you have any questions, do not hesitate to contact us.

The data licensing agreement (DLA) that you will sign is a contract between you and the 'USEMP consortium'.USEMP researchers provide you with the use of DataBait. In return you allow the DataBait providers to use your data for research purposes and to help you to better understand how your data may be used.

The agreement basically means that you agree that:

- *the DataBait providers use your data to do research to empower users of online social networks*
- *your data is used to make inferences to help raise your awareness*
- *you will receive invites for surveys and focus groups*

It also means that you consent to:

- *having the DataBait plugins installed to run the web application*
- *processing of sensitive data, such as data revealing racial, ethnic origin, political opinion, religious or philosophical beliefs, trade-union membership, and those concerning health or sex life, to help users to become aware of what social networks might know about them*

DataBait providers commit:

- *to take utmost care of protecting your data*
- *to delete or anonymise the data as soon as possible, but no later than 3 months after the project stops*

6.7.2 Version B, the long DLA

The normal DLA DataBait users have to agree to is divided in sections. Each paragraph starting with a letter is shown as a separate step in the DataBait registration process and thus in the survey.

USEMP Data License Agreement [7]

The parties:

(1) You, participant of the USEMP research project & user of the DataBait platform and services

(2) [CEA-France / iMinds-Belgium / CERTH-Greece / HWC-UK / LTU-Sweden / VELTI-Greece / SKU Radboud Univertity-Netherlands], provider of the USEMP platform and services, joint data controllers, from hereon called 'USEMP Consortium partners'.

(A) You will install the USEMP DataBait tools, the DataBait-Facebook app and the DataBait web browser plug-in and the DataBait graphic user interface (GUI). The DataBait-Facebook app and the DataBait web browser plug-in will provide access to Your Facebook profile and Your browsing behaviour on Your device(s). These tools will be used by the USEMP consortium partners to collect data that You share on Facebook as well as data collected by the web browser. This data can be data You posted (volunteered data), or data captured by the USEMP tools (observed data). The latter concerns online behavioural data (storing what You did on the Internet and on FaceBook).

(B) You license the use of Your volunteered and observed personal data by the USEMP consortium partners, as gathered by the the DataBait-Facebook app and the DataBait web browser plug-in for the sole purpose of scientific research and – within that context – to provide You through the DataBait graphic user interface (GUI) with information about what third parties might infer based on Your sharing of information, and on Your online behaviour. The said data may be combined with publicly available personal data gained from other sources to infer more information about Your habits and preferences (inferred data).

(C) This license agreement confirms Your explicit consent to store the DataBait tools on Your devices.

(D) The USEMP consortium partners will do scientific research to predict what kind of information Facebook or other third parties with access to Your postings and online behavioural data could or might infer from the said data. These inferences will be shared with You in an intuitive manner, thus providing an online presence awareness tool, embedded in the "DataBait-GUI".

(E) You hereby grant Your consent to process Your sensitive personal data, notably those revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and those concerning health or sex life.

[7]Note that three sections have been deleted from the DLA. These are the reference to estemitating a monetary value with regard to data, participating in qualitative research and lastly reusing data in FIRE. These have been deleted because they are no longer relevant.

(F) The USEMP consortium partners will treat all Your personal data, especially Your sensitive data, with care and delete or anonymize them as soon as possible. Because one of the main goals of the USEMP project is to create awareness about the possibility to infer sensitive data from trivial data trails, it is important to alert You to such inferences and thus to process them.

(G) The USEMP consortium partners will process Your personal data in a secure way and not keep them any longer than necessary for the purpose of the USEMP study. In order to provide You with access to Your personal data and the inferences drawn from them, the data may be kept until the end of the project. Within 3 months of the ending of the research project all personal data will be either deleted, anonymised or processed for related scientific research. In the latter case the relevant USEMP consortium partner will ask You for Your consent.

(H) The national law of Your country of residence (at the moment of registration) is applicable to this contract, assuming you are a resident of the EU.

By clicking continue, you will proceed to the signing of the agreement.

6.8 Annex 8 : Disclosure scoring questions

1. **Your Disclosure Scoring (Likert scale 1=Very Hard, 7=Very Easy)**
   - How easy or difficult was this task?
   - How easy was it to find this function?
   - How difficult was it for you to understand the language and concepts (words) used in this page?
2. **Regarding the accuracy of the most of attributes (Likert scale 1= Not accurate at all, 7=Very Accurate)**
   - In general, how accurate the information provided regarding most of the attributes reflects your personality and habits...
3. **When you see the types of information that could be retrieved from your profile, how much did you worry about who sees this information? (Likert scale 1= Not worried at all, 5=Very Worried)**
   - Facebook friends
   - Facebook Company
   - Future employer
   - State security
   - Advertisers
   - Insurance companies
4. **Do you think that this feature provides a good summary of your disclosed habits/personality? (Yes, No)**
5. **Did you find this feature useful for identifying any potentially sensitive information that you may need to protect? (Yes, No (please specify what was missing)**
6. **If you experienced issues in this page you can describe them here. Feel free to suggest how we could solve this issue in the future.**
7. **Which of these disclosed categories was most surprising? (i.e. you thought you were not disclosing it before but DataBait shows opposite)**
   - Demographics

- Sexuality
- Health
- Hobbies
- Relationship
- Employment
- Psychology
- Politics
- Religion
- None

8. **Did you expect that these kind of information could be retrieved from your profile? Please explain**

After this task respondents were asked to change the sensitivity of their personality traits. This was done via specific instructions we received from our technical partners. After this exercise participants answered the following questions:

9. **Changing sensitivity (Likert scale 1=Very Hard, 7=Very Easy)...**

- How easy or difficult was this task?
- How easy was it to find this function?

10. **How confident are you that you fulfilled this task successfully? (1 = I am not confident at all, 7 = I am very confident)**
11. **If you experienced issues in this page you can describe them here. Feel free to suggest how we could solve this issue in the future**

Lastly, users had to go to the section labelled "Recommended sensitive content"... where a list of posts and likedpages was shown. Theitems in this list havethe highest contribution to the user's overall disclosure score and users are prompted to reconsider sharing these items. This was also followed by a list of questions which concludes the disclosure scoring framework evaluation.

12. **Regarding most sensitive likes and posts (Likert scale 1=Not related at all, 5=Very related)...**
    - To what extent do you think the **liked pages** are related to your most sensitive privacy category?
    - To what extent do you think your **posts** are related to your most sensitive privacy category?
13. **Based on the information provided, have you considered to dislike a page or delete your post? (Yes, No)**
14. **We would like to ask you some questions with regard to the additional information we presented to you during your use of 'your disclosure scoring'**

- How easy or difficult was this information to understand? (1 = very hard, 7 = very easy)
- How likely are you going to use this information if you would want to change something? (1 = very unlikely, 7 = very likely)
- [Open question] If you experienced issues with regard to the provided information, describe them here. Feel free to suggest how we could solve this issue in the future.