D4.9 Privacy transparency

Project	SWELL
Project leader	Wessel Kraaij (TNO)
Work package	WP4
Deliverable number	D4.9
Authors	Bob Hulsebosch (InnoValor), Johanneke Siljee (TNO), Milena Kooij (TNO), Ruud Kosman (InnoValor), Joris Janssen (Sense-OS)
Reviewers	
Date	September 2014
Version	1.0
Access Rights	Internal (project only)
Status	Final

SWELL Partners:

Noldus, InnoValor, Philips, TNO, Radboud Universiteit Nijmegen, Roessingh Research and Development, Sense OS, Almende & Universiteit Twente.

Summary

Smart applications for well-being and –working often consume privacy sensitive data from mobile devices or dedicated sensor sources. Safeguarding privacy is therefore of great concern. Transparency and individual control are bedrock principles of privacy but managing privacy settings in sensor-rich environments and making informed choices about which applications is not trivial.

This deliverable provides an overview of privacy patterns for creating privacy transparency as a first step in achieving sensor data privacy control in a user-friendly manner. Identified privacy transparency patterns are:

- Privacy Policy Text
- Welcome E-mail with Privacy Text
- Privacy Policy Icons
- Q&A list
- Privacy Tutorial
- Personal Data Insight Table
- Personal Data Infographic
- Personal data insight overlay
- Personal data insight on data entry
- Privacy Dashboard
- Privacy Reminder
- Third-party Data Access Notification
- Digital File with Personal Data
- Privacy Awareness Comic
- Privacy Awareness Video
- Video about Transparency
- Transparency Awareness Website
- Transparency Awareness Mobile App
- Advertising Companies graph
- Privacy Transparency label
- Customizable Privacy Transparency label

The privacy patterns are applied to the CommonSense sensor platform in order to select candidate patterns that could be of added value for the enhancement of privacy transparency in the platform. The selected patterns that seemed most promising are:

1. **Personal Data Insight Table Pattern**
2. **Personal Data Insight Overlay Pattern**
3. **Privacy Tutorial**

The patterns will be implemented and evaluated in the remaining activities of SWELL WP4 in 2014 and 2015.

Contents

1 Introduction

Over the course of the last decade, different surveys have taken place to assess users' attitude toward online privacy. Studies consistently report that the majority of the surveyed users (somewhere between 80% and 95%) indicate their concern about their online privacy [1][2][3][4][5][6]. Respondents that indicate not to be concerned about privacy seem not to be well acquainted with possible consequences of losing control over their data, or may have a false sense of safety due to misconceptions on their IT knowledge level [7]. Surprisingly, although a vast majority of respondents reports privacy concerns, users usually do not act accordingly. One would expect privacy to play an important role in users' online behavior given reported concerns; however, Internet users easily provide personal data to web shops or on social networks- a phenomenon known as the privacy paradox. It has been suggested that this might be a consequence of poor understanding of possible risks [7] or of complexity and fragmentation level of privacy related mechanisms [8].

Several studies reported the need for tools that would facilitate easy understanding and some level of control of privacy mechanisms [9][10][11][12][13]. Respondents expressed in [12] they are missing new, easy-to-use technological tools, which would empower users with a sense of control. Several empirical studies have shown that a lower perceived control of personal information release is associated with more privacy concerns [14][15]. Respondents in [12] further added that providing transparency only would already be very much welcome and appreciated. Several researchers have discussed requirements that this type of tools should comply with. To provide such explanation-for-trust these tools should incorporate the right amount and type of information, and present it in an adequate presentation mode, as argued by [10][13]. These authors recognized that even if the information presented is complete and accurate, if it is not understood by users it would not have any positive effect on trust. Although at this moment there exist some tools that provide some pieces of transparency functionality, none of these tools have been designed for the purpose of transparency, they all provide only limited functionality, and are rarely deployed [16][17].

Offering privacy transparency has also been identified as promising for the SWELL context. It aims at giving the user more insight in the data that is shared with applications or other users and for what purposes. We believe transparency is a first step toward privacy control. Once transparency is achieved, other measures can be applied to optimise privacy control.

Particularly for sensor data aggregation platforms like CommonSense, transparency could be of added value as it can increase trust and credibility and enhance its reputation. Moreover, the platform may be in an ideal position to offer enhanced transparency services based on the privacy settings of all its users.

In this deliverable we provide a privacy-by-design solution for providing privacy transparency: privacy transparency patterns. Section 2 gives a high level overview of privacy transparency patterns, and section 3 applies the privacy transparency pattern framework to the CommonSense sensor platform and selects candidate patterns to be implemented by CommonSense. Section 4 draws conclusions and outlines future work.

2 Privacy Transparency Patterns

Privacy design patterns are design solutions to recurring privacy problems; as such they can facilitate the development of privacy-by-design solutions. They are structured according to the software design pattern approach, popular and successful in other areas of software design. Pattern descriptions are aimed at presenting problems and their solutions in a way that humans can understand: when certain problems arise, what the problems are, what to consider when resolving them, how they can be resolved, how their solutions are implemented, and why these solutions are as they are [18].

Privacy design patterns as such exist, but a complete, uniform and readily applicable overview does not exist. We developed such an overview for privacy *transparency* patterns: they focus on solutions on how to create privacy transparency. This section presents that overview. For the sake of readability, we kept the pattern descriptions short, just to give the reader a good idea of what each pattern entails. To make patterns readily applicable, a far more extensive description is required. We will give that description in Section 3, where we describe in detail some of the patterns to be applied in the CommonSense platform.

For the patterns in the overview we use (a selection from) the following topics to give a description of each pattern:

- **Name**: the name of the pattern
- **Goal**: what will be achieved by implementing the pattern
- **Context**: The situation in which the pattern may apply
- **Solution**: the fundamental solution principle underlying the pattern
- **Consequences**: the benefits the pattern provides, and any potential liabilities
- **Examples**: real-world examples of the use of the pattern, if applicable and illustrative.

In chapter 3, we expand the pattern descriptions with:

- **Problem:** what problem the pattern solves
- **Implementation:** how to implement the pattern

We use the following four categories of privacy transparency patterns:

1. **Generic Questions and Answers**: the answers to generic privacy questions that most users have regarding the specific application/service.
2. **Personal Data Tracking**: provide insight to the end-user in how his/her data is handled.
3. **Privacy Awareness**: create awareness at the end-user about the possible privacy risks of sharing personal data.
4. **Privacy Mark**: a seal or certificate given out by a privacy authority that signals to the end user which criteria are fulfilled by the service provider/application.

2.1 Generic Questions and Answers

Providing generic information about an organization's attitude towards privacy can be very useful to the user. This information is relatively static and not dependent on specific user data. Patterns dependent on specific user data are given in see section 2.2.

2.1.1 **Privacy Policy Text**

Goal

To inform the user about a service's privacy policies, and to comply with laws and regulations that require such a document.

Solution

Create a privacy policy document that sets out how the service uses and protects any information that a user discloses while using the service.

How

A downloadable pdf document linked from the service's website.

Where in the flow

A link shown at the start of using the service, but also available somewhere on the website for the user to read at all times.

Consequences

Most users find such a static policy text too long and too complicated to read, so they don't read it at all. Most privacy policies are not read.

2.1.2 **Welcome E-mail with Privacy Text**

Goal

To inform the user about a service's privacy policies.

Solution

A welcome e-mail usually contains information about where to start with the service and possibly where to find documentation, F.A.Q., etc. Such an e-mail can also include information about the service's privacy policy: how a service uses and protects any information that a user discloses while using the service.

How

An e-mail sent to a new user.

Where in the flow

After a new user has registered for the service.

Consequences

A welcome e-mail reaches new users before they start using the service, giving them the chance to get familiar with a service's privacy policy and options, so they can make an informed decision on how their personal data is handled. However, most users will want to start using the service after registration and ignore or only briefly skim through the welcoming e-mail, not reading the privacy text at all.

2.1.3 **Privacy Policy Icons**

Goal

To inform the user about a service's privacy policies.

Solution

The privacy policy icons show how a service uses and protects any information that a user discloses while using the service. These icons effectively show, in a simple graphic language, the most relevant information from a privacy policy text.

How

Multiple icons shown on the service's user interface. Icons should be graphical, and self-explaining: their meaning should be depicted by the pictogram itself. Clicking on an icon brings a pop-up or new window explaining what the icon means. Some possible categories are "Retention Period", "Third Party Use", etc. Colors or numbers can be used to rate or specify a specific item. For example, a retention period of 1 year can be signified using "1Y" within the icon.

Where in the flow

A link shown at the start of using the service, but also available somewhere on the website for the user to read at all times.

Consequences

Icons give users the most important information from a policy text in one glance, especially if they are standardized. Privacy policy texts are not read, icons are easy to see, stand out, and easier to show on smart phone displays than long texts. However, as they only show a portion of the information from the privacy policy, some argue that they decrease transparency instead.

Examples

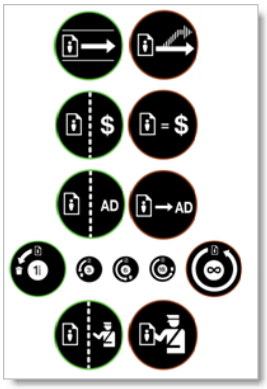


Figure 1: Mozilla Privacy Icons (discontinued)

Figure 2: Kijkwijzer for Dutch television

Figure 3: Creative Common icons

Figure 4: AFM Financiële Bijsluiter

2.1.4 **Q&A list**

Goal

To explain the privacy aspects of personal data usage in the service in a readable format.

Context

You want to qualitative explanation on the most important aspects of data usage in your service. You want to give more background information and room to explain why certain decisions are made in data usage.

Solution

How

A separate page with a standard Q&A list. Questions to be answered are:

- What data is collected?
- To which purpose is data collected?
- What is meant with (informed) consent?
- How is the data stored?
- Who has access to the data?
- How can a user delete her data?
- Etc.

Where in the flow

Available at all times through the menu.

Consequences

A Q&A allows the user to only read the part that is of interest. The challenge is to keep the text readable and still be informative. Too much text might be too boring to read and become

theoretical. It also shows intentions, rather than what actually happens, which could make the user sceptic.

2.1.5 Privacy Tutorial

Goal

To have a step by step guidance on how the service works, what the related privacy issues are, and how users can change their data settings.

Context

If your service is rather complex and a lot of data is gathered, you may want to give users a step by step explanation.

Solution

How

An instructive video in which the user can get acquainted with the service, primarily from the privacy perspective.

An alternative implementation for mobile applications is to let the user swipe through a couple of screens.

Where in the flow

At the start of using the service, or after the user has been using the service for a while and thus has a bit more experience. Also needs to be available on a separate page where possibly multiple short tutorials are accessible, so the user can go back to it.

Consequences

A video is a light-weight, possibly funny way to explain the privacy aspects of a service to users. Users do not have to read long texts, thereby increasing the amount of users reached. Some users might find it too long to go through a whole tutorial, not informing themselves about it at all. The video needs to be of very good quality, entertaining, etc., to keep the user's interest, which is not easy to make and may be expensive to have it made by a professional film maker. Insight in possible consequences might put user at unease of using the service. Therefore it is important to inform the user sufficient measures have been taken to protect his/her privacy.

2.2 Personal Data Tracking

Personal data tracking aims at giving users real-time insight in how their personal data is handled by the service.

Extra care may be given to show the existence of multiple data sensor streams and how they are combined. A single sensor data stream may not be privacy sensitive in itself. However, the combination of multiple streams may become very privacy sensitive. For instance, the information

obtained from heart rate variability and location sensor is much more sensitive than from the individual sensors. It indicates at which places the user is stressed or not. Another example is the combination of location and speed information that can be used by the police to summon the user.

2.2.1 **Personal Data Insight Table**

Goal

To give the user an overview of which personal data is collected, how and why it is used for a service, who has insight in the data, whether their data is disclosed to third parties, etc.

Context

You want to give users insight in what happens with their data because of legislation, to be transparent to your own users.

Solution

How

A table on a separate page that shows the overview. The overview could show:

- Which data
- Why collected
- How used/for which purpose collected
- Who has access to the data
- Who the user authorized for access
- Which consent the user has given for specific data
- To which parties the data is disclosed
- Who has seen the data
- Whether the data can be hidden
- Whether the data can be removed
- How long the data is stored
- How datasets are combined to create richer (privacy sensitive) information
- With which other information the data is combined

Where in the flow

Options are (not mutually exclusive):

- At the service's help section
- At the service's privacy section
- Through a separate menu item
- At a myData section of the service

2.2.2 **Personal Data Infographic**

Goal

To give the user an overview of which personal data is collected, how and why it is used for a service, who has insight in the data, whether their data is disclosed to third parties, etc.

Context

You want to give users insight in what happens with their data because of legislation, and/or to be transparent to your own users. Alternatively, you are an external party that wants to show the privacy consequences of using certain services to a wider group of people.

Solution

How

An infographic (visualization) on a separate page that shows the overview. The overview could show:

- Which data
- Why collected
- How used/for which purpose collected
- Who has access to the data
- Who the user authorized for access
- Which consent the user has given for specific data
- To which parties the data is disclosed
- Who has seen the data
- Whether the data can be hidden
- Whether the data can be removed
- How long the data is stored
- How datasets are combined to create richer (privacy sensitive) information
- With which other information the data is combined

Where in the flow

Options are (not mutually exclusive):

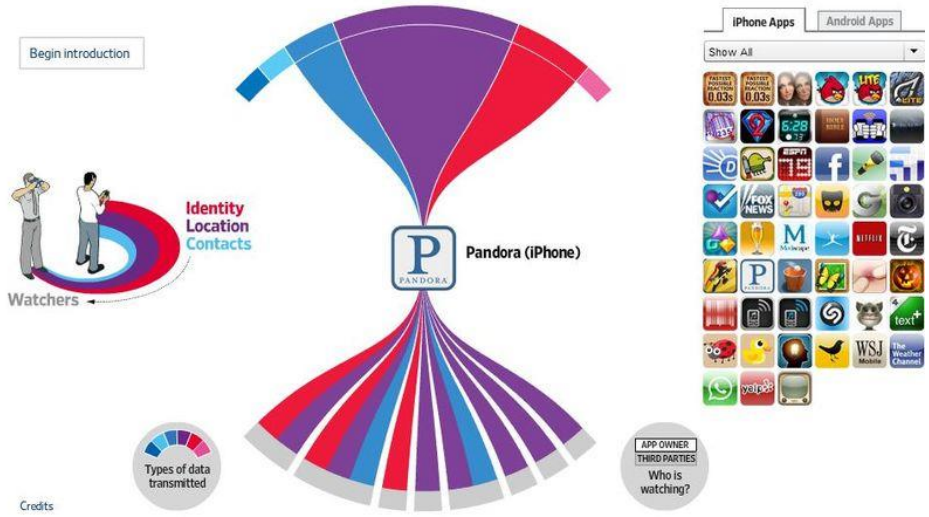
- At the service's help section
- At the service's privacy section
- Through a separate menu item
- At a myData section of the service

The service delivering the infographic depends on the context. It could be made available by an external (independent) party to educate a user about a certain (type of) service and the amount of personal data that is collected. Or it could be made available by the service itself to show users how their data is used.

Example/real uses

Research shows that many of the publicly available smartphone applications are releasing users' private information to online advertisers (e.g. location information) or to developers (e.g. phone

number and SIM card serial number). This is an example from the Wall Street Journal[1] on which personal data from mobile apps is transmitted to third parties.



2.2.3 **Personal data insight overlay**

Goal

To give the user a visual overview of which personal data is visible for other users at that moment.

Context

You want to give users insight in who else as access to their personal data because of legislation, and/or to be transparent to your users.

Solution

How

An overlay over the normal screen which marks the parts of the personal data that is visible by others. Can be fine-tuned by letting the user first select a certain external viewer type or role (e.g. service administrator, researcher, the user's general practitioner). Additionally, information about time of last viewed can be shown.

Where in the flow

Available at all times on screens where personal data is visible. Through clicking on icons for example a different view can be selected.

Consequences

[1] http://blogs.wsj.com/wtk-mobile/ (Visualization not online available anymore)

An overlay gives quick and easy insight in what is viewed by whom. Also can be viewed at all times, directly where personal data is visible. It may also scare users into not providing personal information or even stop using the service.

2.2.4 Personal data insight on data entry

Goal

To give users a warning or immediate insight at the moment they enter personal data in the service (and possibly offer options to change the settings), about aspects like how and why the personal data is used for the service, who has insight in the data, whether their data is disclosed to third parties, etc.

Context

You want to give users insight in who else as access to their personal data because of legislation, and/or to be transparent to your users.

Solution

How

Using icons, or a pop-up, an application can give insight in who else can see the data once it is entered. Double-clicking on a pop-up reveals more detailed information on e.g. what data is used for and who has access to it.

Where in the flow

Whenever a user is required to enter data.

Consequences

Giving insight the moment a user enters data also gives the possibility to withdraw from the submission of data. The link between data entry and making the data available for others is made directly, making it easier to implement user friendly privacy control features. It is not adequate for sensor data collection. User may feel overwhelmed by these insights and refrain from delivering more data, or from using the service at all.

2.2.5 Privacy Dashboard

Goal

To give the user an overview of which personal data is collected, how and why it is used for a service and who else can see the data. Next to transparency, a dashboard offers control features: to let the end-user control who has access to which personal data.

Context

You want to give users insight in who else as access to their personal data because of legislation, and/or to be transparent to your users. The same holds for the control part of the Dashboard.

Solution

How

A dashboard on a separate page that shows both the overview and the control options. What and how the data is shown can be implemented using patterns such as Personal Data Insight Table and Personal Data Infographic.

Where in the flow

Options are (not mutually exclusive):

- At the service's help section
- At the service's privacy section
- Through a separate menu item or webpage

Example

Google Dashboard[2]

2.2.6 Privacy Reminder

Goal

To regularly remind users that their personal data is still processed by the service, as they may forget. Processing incorporates recording, analyzing, storing, and sharing personal data.

Context

Especially relevant for services that continually record a user's personal information (e.g. location, audio, fitness trackers), but also for services that hold personal data in storage. Users may forget that their personal information is processed by a service, and sending a reminder at a regular basis reduces possible privacy risks for users.

Solution

How

Send a reminder by e-mail, SMS, notification in an app, etc. Timing could depend on user activity: if a user has not actively used the service for a certain amount of time, then send the notification.

Consequences

[2] https://www.google.com/dashboard

Users may not be aware that their personal data is still processed by a service. This could pose extra privacy risks, e.g. by a user doing things that he/she would not want to have recorded by the service. To limit the risk of exposure and privacy breaches, personal data that is no longer needed should be removed from a service.

2.2.7 Third-party Data Access Notification

Goal

To notify a user that a third party accessed their personal data within the service. Access includes viewing, editing, copying, analyzing, downloading.

Context

You want to be able to notify your users when someone else accessed their personal data, and who that was. The other party can be another user, external party or even an application. The user may want to be informed of this immediately.

Solution

How

Send an e-mail, SMS, notification in an app, etc. with either only the notification that a user's data has been accessed and that she can see who by going to a certain page or screen, or list names, date and time, which data has been seen, reason, etc. in the notification itself.

This type of notifications should be something that can be turned off and on by the user in the service. Other options are to let the user choose the frequency of such notification (immediate, daily digest, monthly newsletter, etc.), depending on the actual frequency of such events happening.

Alternatively, the service may also notify a user if their data has not been accessed for a long time.

The notification can contain a link to the user's privacy settings, to allow the user to easily change her privacy settings as she may be triggered to do so by the contents of the notification.

Consequences

The advantage of this solution is that it is very simple and cheap to implement. If implemented, it also gives insight in the amount of users that click on a link to change their privacy settings. The drawbacks are that users may start to ignore the notifications in case of high frequency and the lack of 'sexiness' that is inherent to privacy. The challenge is to keep the user's attention after several notifications.

Example

LinkedIn Who's Viewed Your Profile e-mail, TaintDroid[3]

2.2.8 Digital File with Personal Data

Goal

To allow users to request and receive a digital file containing their personal information.

Context

You want to give users insight in what happens with their personal data because of legislation, and/or to be transparent to your users.

Solution

How

Asynchronous: By using a request form on the website or sending an e-mail to e.g. the support desk a user may be able to request a digital printout of her personal information processed and stored by a certain application or organization. The organization then gathers the data and preferably secures and compresses the data (e.g. using zip/rar) to send it to the user, again possibly by e-mail or download server, depending on the size of the file.

Synchronous: alternatively, upon the users request the digital file is automatically prepared and made ready to download or e-mail immediately.

Where in the flow

In the help/support/FAQ part of the application should be a link or text that explains how to request this information.

Consequences

Giving users a digital file, e.g. via e-mail, is a light-weight implementation that does not affect the application's interface at all. It also allows the organization to spend some time gathering the information before actually sending it, similar to responding to support requests, data rectification and data deletion requests.

2.3 Privacy Awareness

Educating users about the privacy risks will create awareness about their privacy and the options they have to control it. Privacy awareness may make users:

- more cautious in releasing personal information within a certain service (which could be a negative consequence for the service);

[3] http://appanalysis.org/index.html

- choose a service that has better privacy protection, perhaps even if that would mean paying for the service;
- pro-actively search for a service's privacy settings and set them to a more privacy-preserving state.

Privacy awareness is of extra importance for sensor-based applications. A single sensor data stream may not be privacy sensitive in itself. However, the combination of multiple streams may become very privacy sensitive. For instance, the information obtained from heart rate variability and location sensor is much more sensitive than from the individual sensors. It indicates at which places the user is stressed or not. Another example is the combination of location and speed information that can be used by the police to summon the user. The challenge is to convey these types of privacy aspects to the user. Often users find it difficult to estimate the privacy risks.

Privacy awareness is typically provided by independent third parties like governmental institutions, schools and universities, non-profit organizations. However, service organizations that want to stand out on excellent privacy behavior may also wish to make their users more privacy aware.

2.3.1 **Privacy Awareness Comic**

Goal

To make the user aware of the privacy risks associated with a certain service.

Context

You want to educate users on the privacy risks of using a certain (type of) service, and do that in a light-weight, funny way. You may be an independent external party, of a service provider.

Solution

A comic that illustrates the privacy risks for the user associated with using a certain service, or the risks of combining multiple data sets.

How

Can be implemented through a pop-up, or a link to a new page or window.

Where in the flow

Options are (not mutually exclusive):

- During registration with a new service
- At start application
- At an external review/help site, that a user visits independently
- At the service's help section

The service delivering the comic depends on the context. It could be made available by an external (independent) party to educate a user about a certain (type of) service and the privacy settings that would be available. Or it could be made available by the service itself to educate users about the service's different privacy options and their respective consequences.

Consequences

A comic is a light-weight, possibly funny way to raise awareness of privacy risks. Users do not have to read long texts, thereby increasing the amount of users reached.

2.3.2 **Privacy Awareness Video**

Goal

To make the user aware of the privacy risks associated with a certain service.

Context

You want to educate users on the privacy risks of using a certain (type of) service, and do that in a light-weight, possibly funny way. You may be an independent external party, of a service provider.

Solution

A video that illustrates the privacy risks for the user associated with using a certain service, or the risks of combining multiple data sets.

How

Can be implemented through a pop-up, or a link to a new page or window, or a link to e.g. YouTube. Could be an animation or live-action movie.

Where in the flow

Options are (not mutually exclusive):

- During registration with a new service
- At start application
- At an external review/help site, that a user visits independently
- At the service's help section

The service delivering the video depends on the context. It could be made available by an external (independent) party to educate a user about a certain (type of) service and the privacy settings that would be available. Or it could be made available by the service itself to educate users about the service's different privacy options and their respective consequences.

Consequences

A video is a light-weight, possibly funny way to raise awareness of privacy risks. Users do not have to read long texts, thereby increasing the amount of users reached. It may reach many viewers if placed on a public video distribution site. Users may not sit out the entire video, and a viewer cannot in one glance see whether a video contains something more interesting in the remainder, unlike text. Insight in possible consequences might put user at unease of using the service. Therefore it is important to inform the user sufficient measures have been taken to protect his/her privacy.

2.3.3 Video about Transparency

Goal

To illustrate what is privacy transparency and what it is not.

Context

You want to make people aware of what privacy transparency is, their rights, how to increase the level of insight in their personal data. You may also want to show the user that a certain service is providing that transparency (combination with Privacy Awareness Video).

Solution

How

A (short) animation or live-action movie explaining privacy transparency in general. Can be implemented through a pop-up, or a link to a new page or window, or a link to e.g. YouTube.

Where in the flow

Options are (not mutually exclusive):

- During registration with a new service
- At start application
- At an external site that a user visits independently, e.g. review/help/blog/YouTube/…
- At the service's help section

2.3.4 Transparency Awareness Website

Goal

Raise awareness and educate users about what is happening to their information when they use specific types of services.

Context

You want to create a website that provides information about what happens to people's personal information. You may represent a consumer organization, a service provider that wants to distinguish itself on privacy, or independent individual.

Solution

How

A website that informs users about what happens to their information when they use privacy invasive services (on the Internet, mobile apps, etc.). May also contain tips, guidelines, or links to external applications that enhance privacy. Not necessarily linked to a specific service.

Examples

Teaching Privacy[4], Me & My Shadow[5]

2.3.5 Transparency Awareness Mobile App

Goal

Raise awareness and educate users about what is happening to their information when they use specific types of services.

Context

You want to create a mobile application that provides information about what happens to people's personal information and what the possible consequences may be (e.g. when combining different data). You may represent a consumer organization, a service provider that wants to distinguish itself on privacy, or independent individual.

Solution

How

A mobile application that informs users about what happens to their information when they use privacy invasive services (on the Internet, mobile apps, etc.). May also contain tips, guidelines, or links to other applications that enhance privacy.

2.3.6 Advertising Companies graph

Goal

To provide transparency on which, if any, advertising and/or behavioral tracking takes place while using a service.

Context

[4] Teaching Privacy
[5] https://myshadow.org/

You want to provide evidence that your organization complies with its privacy policy and not have any tracking parties on your website/mobile app. You would like something made by an independent party to increase the credibility of the evidence.

Solution

How

A visual representation such as a graph that displays the interactions and connections of websites visited and the tracking sites to which they provide information. Can be implemented by using the third-party tracking cookies placed on the user's computer while visiting various websites. The same is possible for mobile applications.

In the graph each dot represents a website. The gray dot in the middle is the visited website (the service itself); the dots connected to the grey dot would be, if existing, the (advertising) sites that have created cookies in users browser and are now tracking his/her behavior on this particular website.

Where in the flow

Options are:

- At the start of the service
- At the service's privacy section
- Available through a menu option

Consequences

May not be easy to interpret for all types of users.

Example

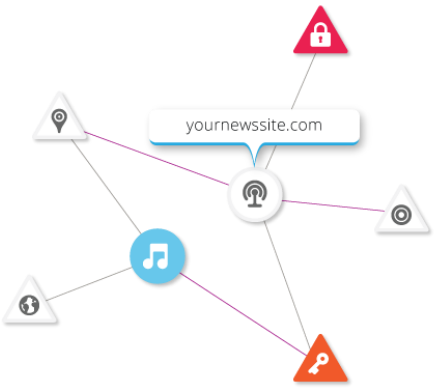


Figure 5: Firefox Add-on Lightbeam[6] uses interactive visualizations to show the first and third party websites a user interacts with on the Internet while the user is browsing.

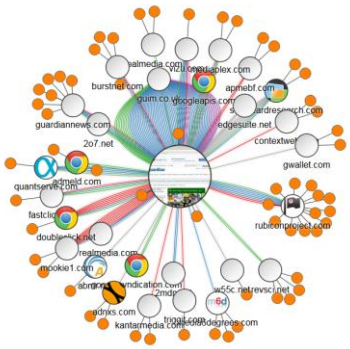


Figure 6: Chrome and Firefox add-on Netograph[7] provides a user with a visualisation of what a website on the 'social web' actually does (in terms of which resources are requested, and by whom, in real-tine) before the user visits it.

2.3.7 **Privacy Settings Trend Detection and Notification**

Goal

To make a user aware of privacy trends, that there may be a good reason to change privacy settings as other users suddenly did. Could be for a specific application or for a wider range of applications (e.g. all mobile applications).

Context

You want to detect situations where several users suddenly change their application's or device's privacy settings. You want to share this information with your other users, to notify them of the trend and allow them to also adjust their privacy settings.

Solution

How

The system monitors privacy setting changes, and is capable of detecting a situation that several users suddenly change their privacy settings, e.g. with respect to a specific external application or third party or other user. Send an e-mail, SMS, notification in an app, etc. with either only the notification that a privacy trend has been spotted and that she can see what is going on by going to a certain page or screen, or give the details of the trend in the notification itself. Also in the case of a compromised external application, the users could be notified about this by the platform.

This type of notifications should be something that can be turned off and on by the user in the service.

The alert can contain a link to the user's privacy settings, to allow the user to easily change her privacy settings as she may be triggered to do so by the contents of the notification.

[6] https://www.mozilla.org/en-US/lightbeam/
[7] http://netograph.com/

2.4 Privacy Mark

A mark gives a sense of trust, especially when given by trustworthy (and independent) institutions. It shows users in a fast way if the service is compliant to legislation.

2.4.1 Privacy Transparency label

Goal

To give a quick insight if the service is transparent about personal data and protects privacy according to applicable legislation.

Context

You do not want your users to have to worry about privacy with each data entry they make. You want your users to feel safe by using your service, and prove you are privacy friendly to attract more users.

Solution

How

A label icon or logo gives insight in to what extent the service deals with data. This should be placed on the header of the service, with a link to the website that explains more about the label and about the institution providing the label.

Where in the flow

Available at all times, but especially on installation, registration, and first use of the service.

Consequences

If multiple labels are circulating, the value of a label is decreasing, as the user will have no idea how the labels differ from each other and what they really mean. The meaning of the label might not fully cover the privacy requirements a user may have, so the user may still need more information.

Examples

Figure 7: EuroPriSe - European Privacy Seal[8]

Figure 8: Logo Privacy Waarborg[9] for direct marketing and sales.

There is a lot of work going into graphical representation of safety levels. However, one should be careful about the meaning of a privacy mark. The meaning of an mark may be obvious for certain (groups of) persons whereas for other (groups of) persons this may not be the case at all. For instance, a recent investigation by SmartHomes showed that standard icons as used everywhere for 'movie' and 'camera' got interpreted as 'loudspeaker' and 'washing machine' by a large percentage (>20%) of responders.

2.4.2 Customizable Privacy Transparency label

Goal

To allow users to match their own privacy/transparency standards with that of a service and to show to what extent the service meets those standards.

Context

You do not want your users to have to worry about privacy with each data entry they make. You want your users to feel safe by using your service, and prove you are privacy friendly to attract more users.

Solution

How

A label icon or logo gives insight in to what extent how the service deals with data matches the preferences of the user. The label should be placed on the header of the service, with a link to the website that explains more about the label and about the institution providing the label. The user can adjust the standards for the label according to her privacy preferences on the website/app of the institution providing the label.

Where in the flow

If not already done, the user is asked if they would like to set their privacy preferences - by going to the label website - on first use or installation of the service. Next, the label indicates to what extent the service matches the user's privacy preferences. In case of a mismatch, the user may decide to

[8] https://www.european-privacy-seal.eu/
[9] https://ddma.nl/wat-doet-ddma/privacy-waarborg/

not use the service, or the service may be able to offer the user the control functionality to disable (some of) the features that cause the mismatch.

Consequences

Users are in more control if they can set the label according to their privacy preferences and decide whether or not to use the service if they see that the service doesn't meet that standard. Also consequences are given which empowers them to decide how they want to proceed. It prevents users from searching for the information, and from using the service without even thinking about the privacy consequences.

Example

Privacy Bird[10] (discontinued) was an add-on for Internet Explorer (IE) that automatically searches for privacy policies at every web site a user visits. It automatically reads policies encoded according to the Platform for Privacy Preferences (P3P) standard, also discontinued, and displays them in an easy to understand language. Privacy Bird matches user's personal privacy preferences with the privacy policy, and notifies the user as to whether her privacy preferences are met by displaying a bird icon in the top right of the title bar of the user's browser.

[10] http://www.privacybird.org/

3 Applying Privacy Transparency Patterns in the CommonSense Platform

CommonSense is a platform that helps users keep track of all their sensor data, store it in a central location, and play with it. CommonSense also processes user's raw sensor data into meaningful things like sleep, exercise, or top locations. With the CommonSense Dashboard (commonsense-dashboard.com) users gain insights into their behavior. With the CommonSense Tracker users turn their phone into an advanced tracking device.

Unconditional user privacy is one of the core values of CommonSense. Users own their data and they can do with it whatever they want. CommonSense applies privacy by design. To evaluate the privacy transparency pattern approach, we compared the set of patterns presented in Section 3 with the current status of the CommonSense platform. Furthermore, some of the relevant patterns have been selected to be additionally implemented in the platform and validated with real end-users.

The table below shows which patterns are implemented by the current (beta) version of the CommonSense platform, which have been selected for implementation, and why.

Table 1: Transparency Patterns in the CommonSense platform. The options and their meaning are as follows. 'Yes': already implemented; 'To do': will be implemented as part of the evaluation; 'No': will not be implemented; and 'n/a': not applicable for the CommonSense platform.

Paragraph nr	Pattern Name	In CommonSense? (Yes, To do, No, n/a)
	Generic Questions and Answers	
3.1.1	Privacy Policy Text	Yes
3.1.2	Welcome E-mail with Privacy Text	Yes
3.1.3	Privacy Policy Icons	No, haven't been able to make good icons
3.1.4	Q&A list	Yes
3.1.5	Privacy Tutorial	To do, exists in the e-coaching app, not yet for the website.
	Personal Data Tracking	
3.2.1	Personal Data Insight Table	To do
3.2.2	Personal Data Infographic	No, too much work

3.2.3	Personal data insight overlay	To do[11]
3.2.4	Personal data insight on data entry	n/a, no manual data entry
3.2.5	Privacy Dashboard	Yes
3.2.6	Privacy Reminder	No, never thought about it so far
3.2.7	Third-party Data Access Notification	No
3.2.8	Digital File with Personal Data	Yes
	Privacy Awareness	
3.3.1	Privacy Awareness Comic	n/a, we are just one product not an organization who should be promoting privacy
3.3.2	Privacy Awareness Video	n/a, we are just one product not an organization who should be promoting privacy
3.3.3	Video about Transparency	n/a, we are just one product not an organization who should be promoting privacy
3.3.4	Transparency Awareness Website	n/a, we are just one product not an organization who should be promoting privacy
3.3.5	Transparency Awareness Mobile App	n/a, we are just one product not an organization who should be promoting privacy
3.3.6	Advertising Companies graph	n/a, we are just one product not an organization who should be promoting privacy
	Privacy Mark	
3.4.1	Privacy Transparency label	No, no label available
3.4.2	Customizable Privacy Transparency label	No, no label available

[11] This functionality is actually already available, just not on the main view because it would too much info there. On the main sharing view of CommonSense the user can exactly see to which data others have access.

By going through all the transparency patterns, it became apparent that especially the Personal Data Tracking solutions are still missing in the application, as can be seen from Table 1. To be able to evaluate which of the Personal Data Tracking solutions would fit the platform and its users best, we selected two patterns to incorporate in the system's design and implementation:

1. Personal Data Insight Table. In two versions: one version with only a selection of the personal data, and one version showing as much personal data as possible.
2. Personal Data Insight overlay. This pattern will be incorporated in the already existing Dashboard.
3. Privacy Tutorial. This pattern is incorporated in the CommonSense app, but not yet in the CommonSense website.

The sections below contain the full pattern description of these two transparency patterns.

3.1 Personal Data Insight Table Pattern

Goal

To give the user an overview of which personal data is collected, how and why it is used for a service, who has insight in the data, whether their data is disclosed to third parties, etc.

Context

You want to give users insight in what happens with their data because of legislation, to be transparent to your own users.

Type of user

Especially useful for IT literate users that are used to viewing tables and understand which type of data is which.

- Healthy people: to see what data is collected and how it is used and disclosed, and to analyze their data;
- Office workers: to see what data is collected and how it is used and disclosed;
- People with chronic illness: to see their medical data and how it is used, and what caretakers and other organizations can see;
- Sports(wo)men: to see what data is collected and how it is used and disclosed, and to gain insight in their own sports behavior;
- Health freaks: to see what data is collected and how it is used and disclosed, and to gain insight in their own health behavior.

Context requirements:

User context:

- Required is a visual display that is large enough to show the table. A computer, laptop, or tablet screen is ideal; a smart phone may be too small.

Service context:

- It must be possible to structure the data to be able to present it in a table in a usable fashion. It is not useful to show millions of continuous measurements.

Problem

The service wants to give the user insight in the actual personal data that it is processing. This information needs to be accessible real-time for the user, and provided automatically.

Solution

How

A table on a separate page that shows the overview. The overview could show:

- Which data
- Why collected
- How used/for which purpose collected
- Who has access to the data
- Who the user authorized for access
- Which consent the user has given for specific data
- To which parties the data is disclosed
- Who has seen the data
- Whether the data can be hidden
- Whether the data can be removed
- How long the data is stored
- With which other information the data is combined

Where in the flow

Options are (not mutually exclusive):

- At the service's help section
- At the service's privacy section
- Through a separate menu item
- At a myData section of the service

Type of information

A table can show a lot of information or can be adjustable by the user to tweak which information to show, and which values (e.g. which range). From the table links to applicable other pages/screens can be given, to allow a user to easily change privacy settings or visit websites of data buyers.

A way to present more detail than visible at the overview table is to apply the Overview beside Detail[12] user interface pattern.

Implementation

[12] http://www.cs.helsinki.fi/u/salaakso/patterns/Overview-beside-Detail.html

A functional design and proof-of-concept implementation will be made in Q4 of 2014.

Consequences

The pattern has the following benefits.

- A table shows the information in a structured way that is easy to comprehend.
- A table is relatively easy to implement
- Openness to users increases user trust and user participation, and in the long run increases user base and thereby financial income.
- Users will pro-actively search for the service's privacy settings and set them to a more privacy-preserving state, and delete data that is not required for service usage anymore, increasing their own privacy and limiting the privacy-related risks of e.g. an external attack on the service.

The pattern has the following liabilities.

- Users may be put off by seeing how much of their personal data is collected, processed and disclosed to third parties. Users may delete data that would otherwise have been useful for analysis purposes, or stop using the service at all.

These two lists of consequences have to be completed and verified during implementation and end-user validation activities in SWELL that are planned for Q4 in 2014 and Q1 in 2015.

Example

Data	Used for	Visible to	Consent given?	Seen by	Third parties?	Possible to hide?	Removable?
User name	Authentication, authorisation, keeping track of user's behaviour	Administrator, user, user's connections within the service	Yes (with date)/no	Dr. Jones, September 8 2014, 10:06 AM	Yes/No/Which	Not from the system, but possible to hide from user connections	Yes/No, by yourself or by sending a request to us

Other patterns

Personal Data Insight Infographic, Personal Data Insight Overlay

3.2 Personal Data Insight Overlay Pattern

Goal

To give the user a visual overview of which personal data is visible for other users at that moment.

Context

You want to give users insight in who else as access to their personal data because of legislation, and/or to be transparent to your users.

Type of user

Especially useful for people that want to have a quick overview of what can be viewed by other users that are interacting with the service

- Healthy people: to see what other organizations, friends, or other people can see;
- Office workers: to see what their colleagues, doctors and superiors can see, and at which date and time viewing took place;
- People with chronic illness: to see what caretakers and other organizations can see;
- Sports(wo)men: to see what other sports(wo)men and trainers can see;
- Health freaks: to see what organizations can see.

User context

- A larger screen to use the service, as an overlay requires some overview

Problem

The service wants to give the user insight in who else has had access to the user's personal data, including date and time. This information needs to be accessible real-time, provided automatically.

Solution

Type of information

An overlay gives an impression of what is viewed by other users. Depending on the service this can be user profiles, or specific names of doctors.

How

An overlay over the normal screen which marks the parts of the personal data that is visible by others. Can be fine-tuned by letting the user first select a certain external viewer type or role (e.g. service administrator, researcher, the user's general practitioner). Additionally, information about time of last viewed can be shown.

Where in the flow

Available at all times on screens where personal data is visible. Through clicking on icons for example a different view can be selected.

Implementation

A functional design and proof-of-concept implementation will be made in Q4 of 2014. As already mentioned in Table 1 CommonSense already has sharing information available on the main sharing view. It allows the user to exactly see to which data others have access. The focus of the implementation will be mainly on optimizing the user experience and intuitiveness of the overview.

Consequences

The pattern has the following benefits.

- An overlay gives quick and easy insight in what is viewed by whom.
- An overlay can be viewed at all times, directly where personal data is visible.

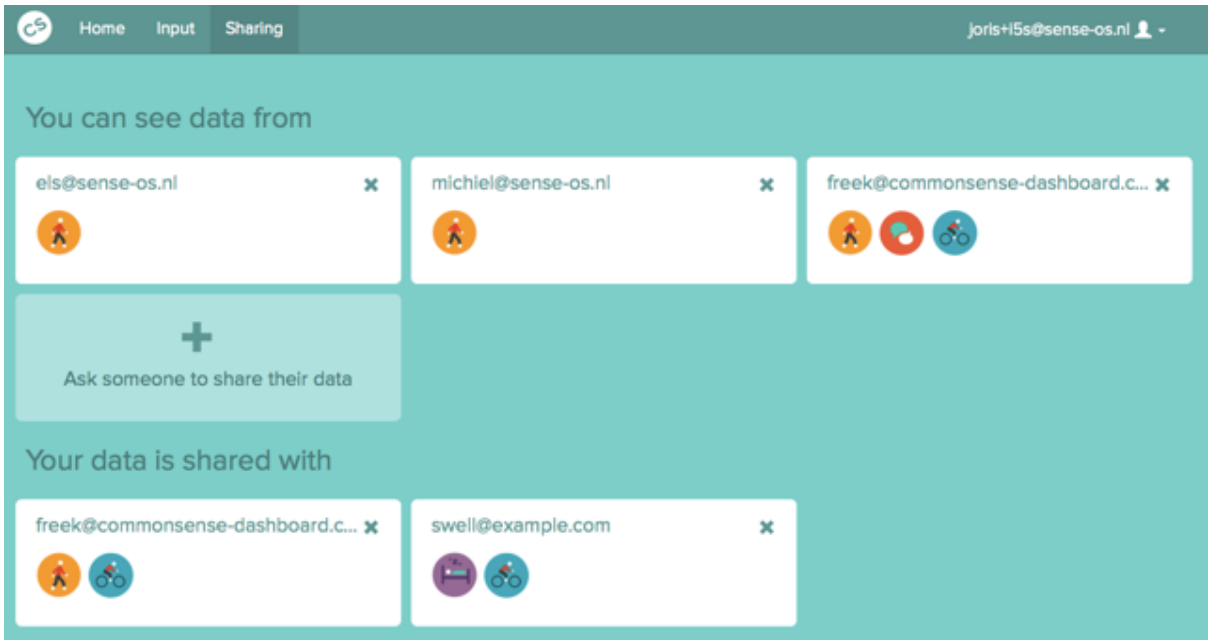
The pattern has the following liabilities.

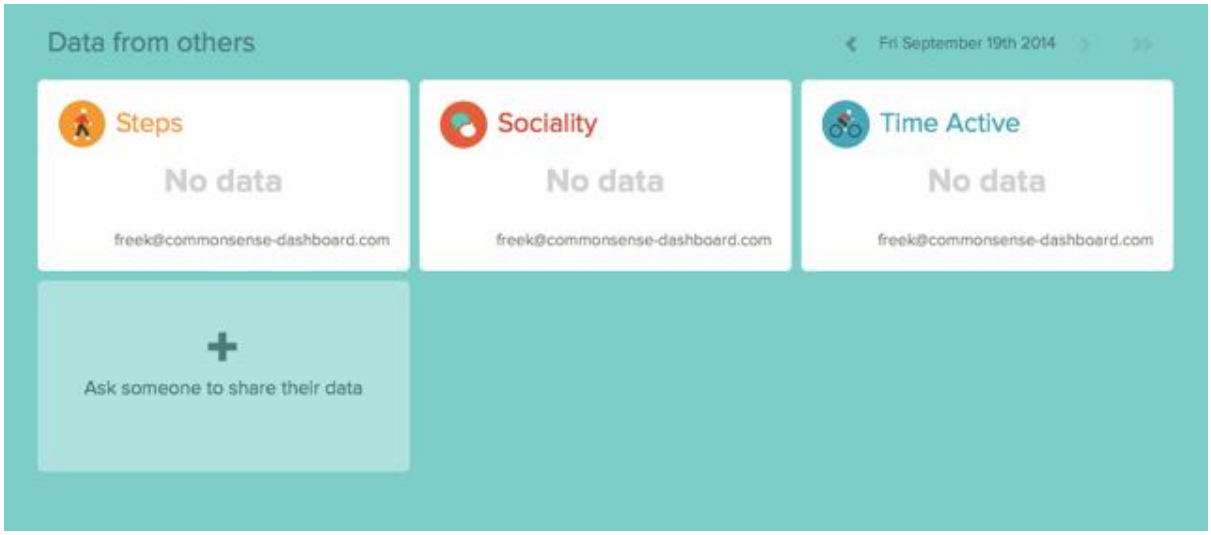
- An overlay may not be able to show the required level of detail.
- Users may be put off by seeing how much of their personal data is viewed by others. Users may delete data that would otherwise have been useful for analysis purposes, or stop using the service at all.

These two lists of consequences have to be completed and verified during implementation and end-user validation activities in SWELL that are planned for Q4 in 2014 and Q1 in 2015.

Example

The figures below shows the current CommonSense implementation of the Personal Data Insight Overlay Pattern.





Other patterns

Personal Data Insight Table, Personal Data Insight Infographic

3.3 Privacy Tutorial

Goal

To have a step by step guidance on how the service works, what the related privacy issues are, and how users can change their data settings.

Context

If your service is rather complex and a lot of data is gathered, you may want to give users a step by step explanation.

Type of user

Especially useful for people that have limited experience with this type of services and need more information on the privacy aspects.

Solution

How

An instructive video in which the user can get acquainted with the service, primarily from the privacy perspective.

An alternative implementation for mobile applications is to let the user swipe through a couple of screens.

Type of information

Information on what data is collected and what for, and who can view data, to which parties the data is disclosed, and possibly privacy consequences of entering specific types of data.

Where in the flow

At the start of using the service for the first time, or, if the user chooses to dismiss the tutorial, after the user has been using the service for a while and thus has a bit more experience. Also needs to be available on a separate page where possibly multiple short tutorials are accessible, so the user can go back to it.

Implementation

A functional design and proof-of-concept implementation will be made in Q4 of 2014.

Consequences

The pattern has the following benefits.

- A video is a light-weight, possibly funny way to explain the privacy aspects of a service to users. Users do not have to read long texts, thereby increasing the amount of users reached.
- Taking the user by the hand helps in creating trust, and a slow pace in getting acquainted with how the service works, how data is used and where the user has control.

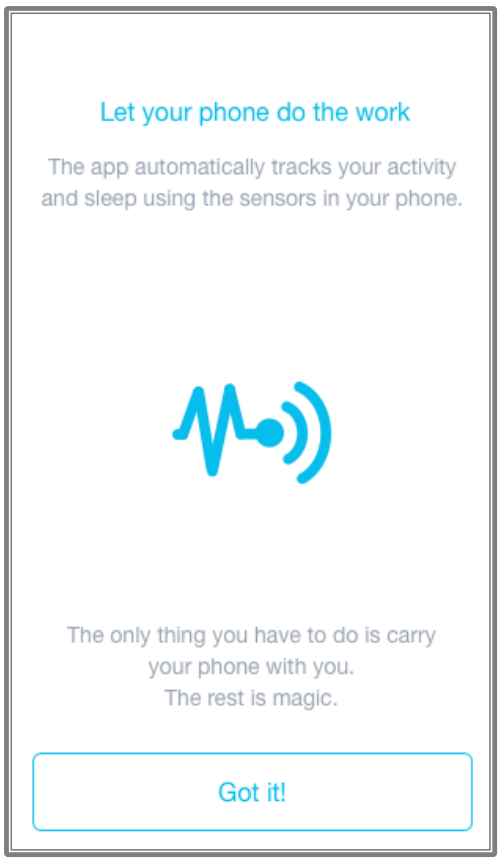
The pattern has the following liabilities.

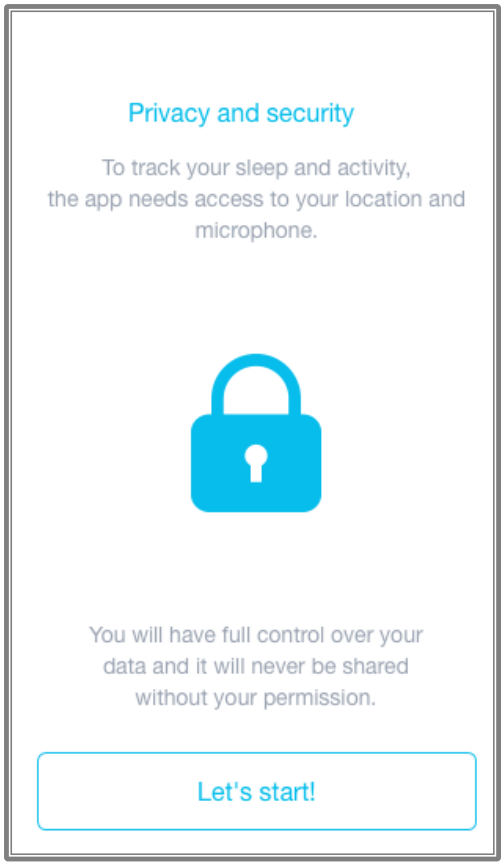
- Some users might find it too long to go through a whole tutorial, not informing themselves about it at all.
- The video needs to be of very good quality, entertaining, etc., to keep the user's interest, which is not easy to make and may be expensive to have it made by a professional film maker.
- Insight in possible consequences might put user at unease of using the service. Therefore it is important to inform the user sufficient measures have been taken to protect his/her privacy.

These two lists of consequences have to be completed and verified during implementation and end-user validation activities in SWELL that are planned for Q4 in 2014 and Q1 in 2015.

Example

The current CommonSense app informs the user about privacy prior to installation of the app. The user has to click through a small number of information screens and one of them is about privacy. The privacy and another screen are shown below.





Other patterns

Q&A List, Privacy Policy Icons

4 Conclusions

The ambition to strive for more user control and transparency regarding the disclosure of privacy sensitive data is not trivial. The ability to provide users with the transparency over what happens to their personal data is a first step towards enabling full control for users over their personal data.

Solutions for providing some form of privacy transparency exist, but no standard approaches. Every application developer who wants to provide some form of transparency builds his own solution, making the same mistakes as others and sometimes resulting in a user interface that is too crowded or just makes users too anxious to use the application at all.

The approach from the software engineering world to collect and make openly available design best practices is called software design patterns. Software design patterns are hugely popular among software developers. To provide the privacy-by-design software engineer with the best practices of privacy transparency, this deliverable presents an overview of privacy transparency patterns. We introduced the following four categories of privacy transparency patterns

1. **Generic Questions and Answers**: the answers to generic privacy questions that most users have regarding the specific application/service.
2. **Personal Data Tracking**: provide insight to the end-user in how his/her data is handled.
3. **Privacy Awareness**: create awareness at the end-user about the possible privacy risks of sharing personal data.
4. **Privacy Mark**: a seal or certificate given out by a privacy authority that signals to the end user which criteria are fulfilled by the service provider/application.

To demonstrate and validate its usage, the transparency patterns will be used to implement privacy transparency in the CommonSense application. As with software design patterns, the software engineer chooses those patterns that provide the best solution to the problems he needs to solve. In this case, three transparency patterns were selected as most suitable for the CommonSense platform, and those were described in more detail:

1. **Personal Data Insight Table Pattern**
2. **Personal Data Insight Overlay Pattern**
3. **Privacy Tutorial**

In the remaining SWELL WP4 activities, the transparency patterns will be implemented and validated with end-users. This feedback will be incorporated in the pattern descriptions.

Other future work will consist of developing a method or framework for selecting privacy patterns that cover the needs of the user and meet the requirements or constraints of well-being applications.

5 References

[1] The Gallup Organization, 'Confidence in the information society: analytical report'. Flash EB FI 250, http:// ec.europa.eu/public_opinion/flash/fl_250_en.pdf, Accessed July 07, 2014.

[2] L. Rainie, 'Transportation and privacy in the mobile age', Pew Internet & American Life Project, January 25, 2012, http://www.slideshare.net/PewInternet/transportation-and-privacy-in-the-mobile-age, Accessed on July 7, 2014.

[3] N.K Malhotra, S. Kim, and J. Agarwal, 'Internet Users' Information Privacy Concerns (IUIPC): The Construct, the Scale, and a Causal Model', Information Systems Research, Vol. 15(4), Dec. 2004, pp. 336-355.

[4] C. Paine , U-D. Reips, S. Stieger, A. Joinson, and T. Buchanan, 'Internet users' perceptions of 'privacy concerns' and 'privacy actions''. International Journal of Human-Computer Studies, Vol.65(6), June 2007, pp.526-536.

[5] S. Bellman, E. Johnson, S. J. Kobrin, and G. L. Lohse, 'International Differences in Information Privacy Concerns: A Global Survey of Consumers'. Information Society, Vol. 20, no. 5, 2004, pp. 313-324.

[6] H. Cho, M. Rivera-Sanzhez, and S.S. Lim, 'A multinational study on online privacy: global concerns and local responses'. New Media Society, vol. 11(3), May 2009, pp. 395-416.

[7] S. Flinn and J. Lumsden, 'User perceptions of privacy and security on the web,' in The Third Annual Conference on Privacy, Security and Trust (PST 2005).

[8] L.F. Cranor, 'Self-defense: it is difficult to protect privacy even if you know how', MIT Technology Review, April 23, 2014.

[9] E. Costante, J.I. den Hartog, and M. Petkovic: 2011, 'On-line trust perception: what really matters'. Proceedings of the First Workshop on Socio-Technical Aspects in Security and Trust, STAST'11, Milan, Italy, September 8, 2011, pp. 52-59.

[10] A. Kini and J. Choobineh, 'An Empirical evaluation of the factors affecting trust in web banking systems,' in Americas Conference on Information System, 2000, pp. 185–191

[11] M. Koufaris and W. Hampton-Sosa, 'The development of initial trust in an online company by new customers'. Information & Management, Vol. 41, Issue 3, Jan. 2004, pp. 377–397; S-J. Yoon, "The Antecedents and Consequences of Trust in Online Purchase Decisions," Journal of Interactive Marketing, Vol. 16 (2), 2002, pp. 47–63.

[12] L. Rainie, 'Privacy Online: How Americans feel… the ways they are responding to new threats … and why they are changing their online behavior', Pew Internet & American Life Project, March 11, 2005, Accessed on July 7, 2014.

[13] W. Pieters,, 'Explanation and trust: what to tell the user in security and AI'. Ethics and Information Technology, Vol. 13(1), 2011, pp.53–64.

[14] H. Xu, 'The Effects of Self-Construal and Perceived Control on Privacy Concerns'. Proceedings of 28th Annual International Conference on Information Systems (ICIS), Montréal, Canada, 2007.

[15] C. Hoadley, H. Xu, J.J. Lee and M.B. Rosson, 'Privacy as Information Access and Illusory Control: The Case of the Facebook News Feed Privacy Outcry'. Electronic Commerce Research and Applications, 9(1), 2010, pp 50-60

[16] M. Janic, J.P. Wijbenga and T. Veugen, 'Transparency enhancing tools (TETs): an overview', STAST2013, New Orleans, 2013,

[17] H. Hedbom, "A Survey on Transparency Tools for Enhancing Privacy", The Future of Identity in the Information Society, IFIP AICT, vol. 298, Springer, Heidelberg, 2009, pp. 67–82.

[18] Markus Schumacher, Eduardo Fernandez-Buglioni, Duane Hybertson, Frank Buschmann, Peter Sommerlad, *Security Patterns: Integrating Security and Systems Engineering*, John Wiley & Sons, 2006.