Kortesniemi, Yki; Lappalainen, Tuomas; Salka, Fayez

User Attitudes towards Consent Intermediaries

Published: 12/12/2018

User Attitudes towards Consent Intermediaries

Yki Kortesniemi
Department of Computer Science,
Aalto University, Finland
Yki.Kortesniemi@aalto.fi

Tuomas Lappalainen
Faculty of Art and Design,
University of Lapland, Finland
tuolappa@ulapland.fi

Fayez Salka
Department of Computer Science,
Aalto University, Finland
Fayez.Salka@aalto.fi

Abstract

Consent intermediaries are an emerging approach to providing individuals better control over how their personal data is used and better tools for re-using the data from one service in other services by collecting all the required management in one place. To understand how individuals feel about consent intermediaries and how they should be developed, the authors implemented a simple UI according to the principles of one of the approaches, MyData, and performed user tests (n=23), where users were asked to manage data sharing between services. Our findings show that there is a clear need for such tools and the consent intermediary approach shows promise.

Author Keywords
Consent, Consent Intermediary, Personal Data, MyData, Legal Design

I. Introduction

Currently many services collect and process detailed personal information about their users. For the users this can mean improved service, but it also means a threat to their privacy unless they can properly control, what is being processed and how. The General Data Protection Regulation (GDPR) (European Union, 2016) states that personal data may only be processed based on one of the six grounds, one of which is the consent of the individual. In this informed consent approach, which is also used in many other jurisdictions, people are expected to manage their privacy by weighing the subjective costs and benefits of data collection in each case (Solove, 2013).

So theoretically the user has a lot of control, but in practice there are a number of obstacles stemming from the complicated process of consenting and the amount of knowledge required for an informed decision (Lehtiniemi & Kortesniemi, 2017). Individuals are often not informed enough because they e.g. do not read privacy policies (Custers, 2016) or make too optimistic assumptions about them (Turow et al., 2015). According to a recent Eurobarometer, only 18% reported reading privacy policies fully and 49% partially, and people felt a lack of control over their personal data (European Commission, 2015). Many individuals even routinely just accept consent dialogues without even reading any information (Böhme and Köpsell, 2010).

To address these problems, the consent intermediary approach tries to empower users to better manage their privacy by collecting the management of all service-related consents (and through them, user's privacy) into a single service. Just having all the consents in one place makes it easier to compare them, but the true potential of the approach is that it facilitates the building of new tools that help people make better informed decision, help simplify the consent management process, and potentially shift the balance of power between the services and users more to the benefit of the users. (Lehtiniemi and Kortesniemi, 2017) Examples of such intermediaries include commercial service developers such as the personal cloud server Cozy Cloud (2018) and the personal information control services digi.me (2018) and Meeco (2018), as well as research-originated initiatives such as the networked personal data indexing device Databox (Chaudhry et al., 2015), personal data stores Hub of All Things (2018) and OpenPDS (de Montjoye et al., 2014), and the personal data management model MyData (Poikola et al., 2015).

To better understand how these intermediary services should be designed to benefit the users, the authors implemented a UI for a MyData-type consent intermediary that facilitated sharing data between health-related services and then performed a qualitative user study (n=23) with non-technical users to understand, how they felt about the current situation and the change a consent intermediary could bring, and what they looked for / worried about in a consent intermediary approach. Specifically, this paper looks at the consent intermediary from the individual's point of view and asks the following research questions:

RQ1. How happy are users about their control over how personal data about them is used in different services and what kind of new tools would they like to have?
RQ2. How do users feel about the consent intermediary approach?
RQ3. How do users feel about a detailed vs simplified (recommendation-based) sharing settings?
RQ4. How do users feel about a list view vs a more visual presentation of the data sharing connections?

The rest of the paper is organised as follows: Section II describes the methodology of the study, Section III presents the results and Section IV discusses the findings.

II. Methodology

The consent intermediary concept was evaluated by first developing a prototype app of a consent intermediary for sharing health data between services and then performing a user study, which consisted of a pre-questionnaire, three tasks with the prototype, a semi-structured interview after the tasks, and optional drawing tasks. The app was designed with two alternative views for the connected services and two alternative consenting views to facilitate research questions 3 and 4.

User Study Design

The pre-questionnaire included basic demographics and questions about previous usage of health tracking apps and data sharing. The participants then used the prototype with an Android tablet (Samsung Galaxy 10) as shown in Figure 1. Before the tasks participants received a short introduction to the concept of a consent intermediary and MyData. Participant were given tasks, which included connecting a running tracking application they had been using for some time to the consent intermediary service and then sharing the running data to a new diary application they had just started using, managing existing data sharings between services, and finally revoking an existing data sharing consent. During the task the users were asked to compare the two alternative views for editing the consent settings and two alternative views of the services and their data sharings. Participant were encouraged to think-aloud during the tasks and describe their actions during interaction with the prototype.

After the tasks with the prototype, a semi-structured interview was conducted where the participants told their thoughts about using the application and possible improvement ideas. There was also discussion about MyData and having the ability to control their own data, as well as hopes and/or worries related to the topic. Finally, a voluntary drawing task was administered where participants could propose and draw improvements to the concept and its design.

Throughout performing the tasks the participants were observed and notes were taken by the study facilitator. Participants' comments and the conversation with the facilitator were recorded and studied in the analysis phase.

Participants

Altogether 23 (19 females, 3 males) participants were recruited from a Finnish university campus area. Participants' backgrounds were mostly from non-technical field, design being the most common, and they all had no prior knowledge of the consent intermediary or MyData concept. The age of the participants varied between 21 -40 yrs (mean: 27 yrs). Related to research interest, participants were asked about their previous use of their personal data and also their previous use of applications that utilize data or personal data.

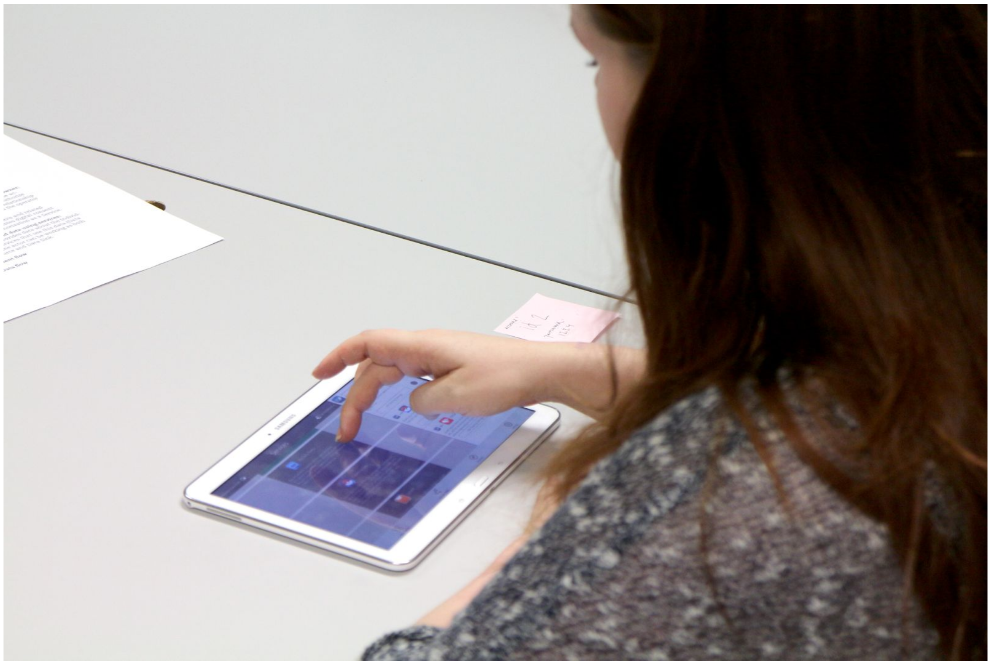


Figure 1. Participant interacting with the prototype during the user study.

Test scenario

The prototype app was designed to let the user manage the sharing of their data between different services. Those services could be anything that processes personal data, but in the test scenario all services were health related. A consent intermediary could also provide functionality for controlling the processing within a service, but this test focused only on sharing data between services due to such functionality being less common at the moment. Also, many of the views and controls used for consenting are very similar both for the processing within a service and sharing between services, so testing both at this stage would have been mostly redundant.

The app needed to be able to provide the users with an overview of the service and data sharing between them, and to be able to scale to complex situation where the user ends up with a large number of services and connections. To this end, the services could be viewed both in a traditional list view (*MyServices*) and a more graphical *Circular View*. In the test, the users were then asked to compare the views.

The user has to have the ability to use the app to control the sharing in sufficient details, so when the user gives consent to their data to be shared between two services, the user should have a good idea about what types of data are being used, and for what purposes they are being processed by the service. For that we composed two kind of views where each consent contains different purposes for data sharing (Figure 2.) and each purpose contains the user data required by that purpose.

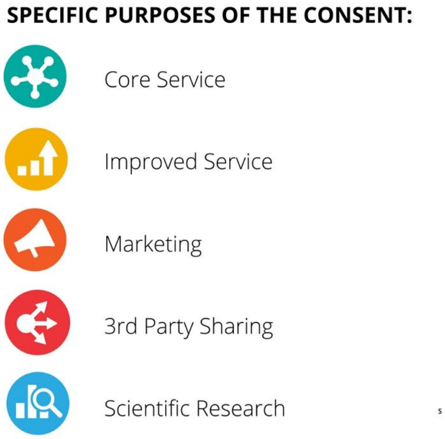
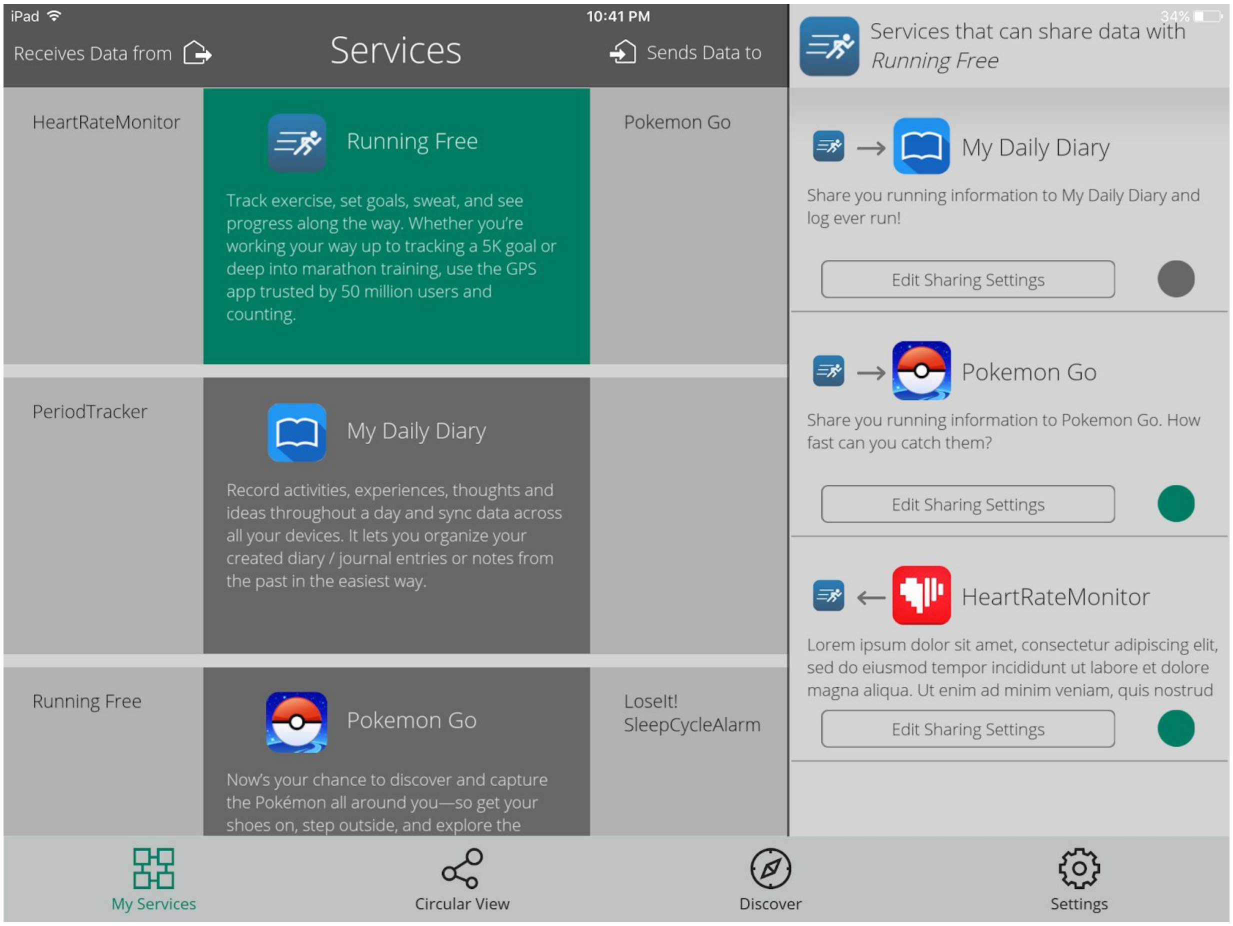


Figure 2: Icons for the different purposes of processing

Design of the test app

The test app consists of the two alternative views to the same information: *MyServices* and *Circular View.* They both show all the services the user has added to the consent intermediary account (the consent intermediary can only control those services the user has added to their consent intermediary account). MyServices view shows the services in a list format (Figure 3.) while the Circular View gives a more visual presentation of the data sharing connections between services (Figure 4.). The MyServices (list) view shows a short description of the service and if the user has consented to data sharing with the service, the connected services are shown on the left and right side columns (receiving data from and sending data to, respectively). In the circular view, all services are represented with small circles and the description of the selected service is shown below, while the data sharing is shown as lines connecting the services so that the color of the line indicates the direction of data flow.



Track exercise, set goals, sweat, and see progress along the way. Whether you're working your way up to tracking a 5K goal or deep into marathon training, use the GPS app trusted by 50 million users and counting.

Record activities, experiences, thoughts and ideas throughout a day and sync data across all your devices. It lets you organize your created diary / journal entries or notes from the past in the easiest way.

Now's your chance to discover and capture the Pokémon all around you—so get your shoes on, step outside, and explore the

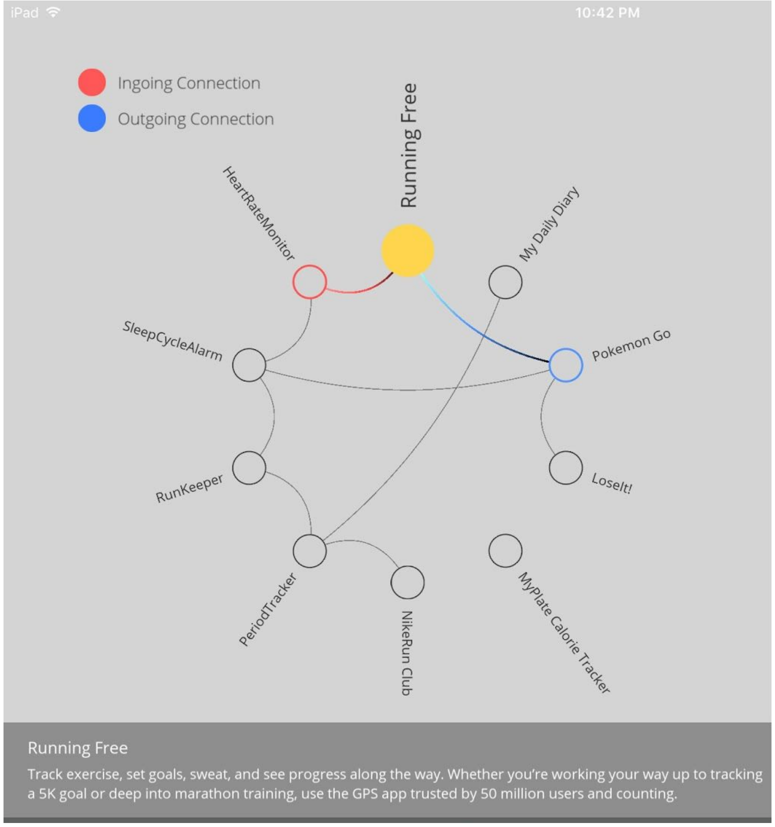
Share you running information to My Daily Diary and log ever run!

Share you running information to Pokemon Go. How fast can you catch them?

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud

Figure 3. MyServices view and the Compatible Services List

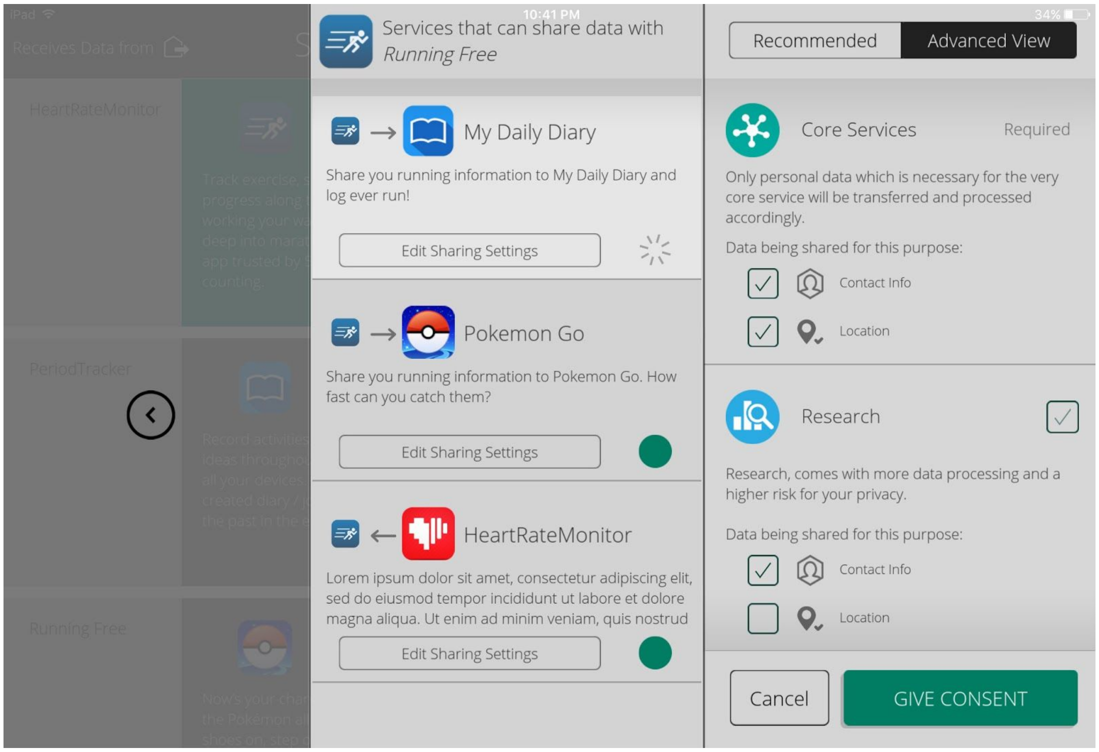
To the right of both the MyServices and Circular views is the Compatible Services list, i.e. all services that can share data with the service currently selected in the MyServices/Circular view. Again, the direction of the arrow between the icons represents the direction of the data flow.



Running Free

Track exercise, set goals, sweat, and see progress along the way. Whether you're working your way up to tracking a 5K goal or deep into marathon training, use the GPS app trusted by 50 million users and counting.

Figure 4. Circular View



Services that can share data with *Running Free*

→ My Daily Diary

Share you running information to My Daily Diary and log ever run!

Edit Sharing Settings

→ Pokemon Go

Share you running information to Pokemon Go. How fast can you catch them?

Edit Sharing Settings

← HeartRateMonitor

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud

Edit Sharing Settings

Recommended | Advanced View

Core Services — Required

Only personal data which is necessary for the very core service will be transferred and processed accordingly.

Data being shared for this purpose:

☑ Contact Info

☑ Location

Research ☑

Research, comes with more data processing and a higher risk for your privacy.

Data being shared for this purpose:

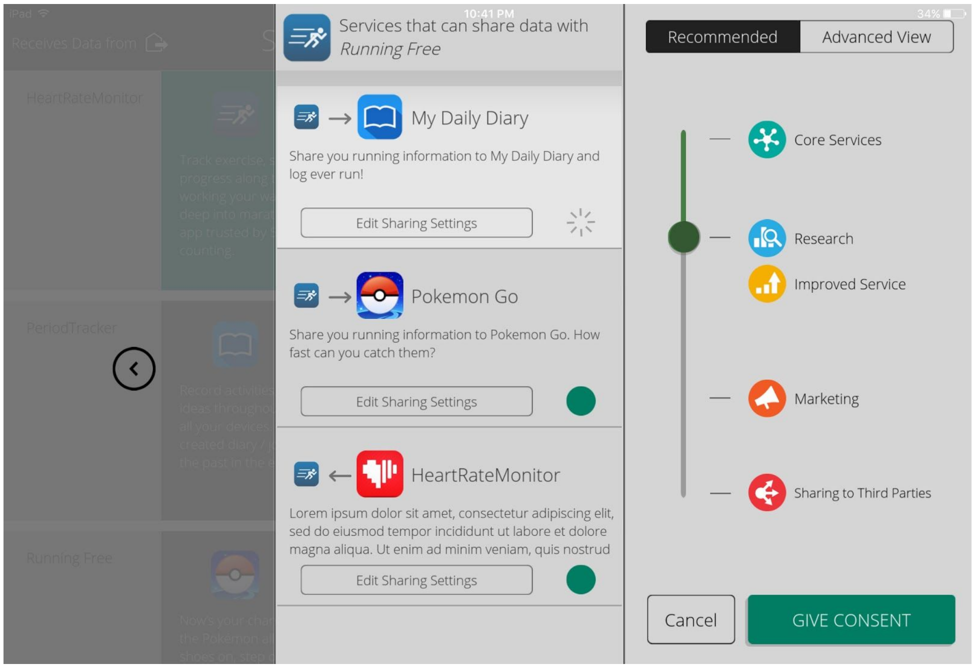
☑ Contact Info

□ Location

Cancel | GIVE CONSENT

Figure 5. The Compatible Services list and the Advanced consenting options view

When the user wants to share data between the services, they click the corresponding 'Edit sharing settings' button and are presented with the options for that data flow. There are two alternative views for deciding the sharing settings: the Advanced view (Figure 5), which gives the user a detailed manual control, and the Recommended (slider) view (Figure 6), which gives a simplified slider.



Services that can share data with *Running Free*

My Daily Diary

Share you running information to My Daily Diary and log ever run!

Pokemon Go

Share you running information to Pokemon Go. How fast can you catch them?

HeartRateMonitor

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud

Figure 7. The Compatible Services list and the Slider consenting options view

The slider is an attempt to provide a simplified consenting view. The idea is that it has been created by a trusted 3rd party chosen by the user, not the services in question, and represent recommended options for the user. The details for each slider position (e.g. which data types are shared for each purpose))are available by clicking the position.

Regardless of the consenting view, once the user is happy with the settings, they can click the Consent button, which enables the data flow. The user is, of course, free to change or even revoke the consent at will.

III. Results

This section presents the findings from the pre-questionnaire, user tests, semi-structured interviews and optional drawing tasks organised according to the five research questions. All participant counts reported are out of 23.

RQ 1: How happy are users about their control over how personal data about them is used in different services and what kind of new tools would they like to have?

In the pre-questionnaire, the participants were asked about their practices related to controlling their data. 7 (out of 23) participants reported they didn't read the terms of service or privacy policy before installing an application, as one participant explained: "the texts are too long to read and when I'm downloading an app I just want to take it into use" (#3). This reflects the findings of previous research, which reported that those who don't read privacy statements often find them too long to read (European Commission, 2015). Some participants did occasionally read the policies when they had an explicit reasons: "if the app look suspicious, I will (read it)"(#10) or "If the applications needs to use my photos or contacts I tend to read the privileges or permissions" (#23).

Participants were interested in how their personal data is shared and used. 16 participants felt that they can sufficiently control their data and some of them said that the control is up to user's own actions e.g. they won't share medical data or any similar sensitive data, and one participant disabled geolocation as a way to control personal data collection. 3 participants mentioned explicitly that they are particularly careful when it comes to health data: "I can live with the idea that applications can have control to my common data. Another thing is medical (i.e. medication) data that I'm not going to give to anyone." (#9). The 7 participants who felt they cannot control data sharing, stated that they want to control specifically where and how data is shared. 4 participants wanted even more information about the sharing and 2 participants wanted to receive weekly or monthly reports to see how and where their data is being shared. Finally, 4 participants wanted to know more about the benefits of sharing data and 4 participants expressed that they don't trust companies on how they handle data.

A few participants wanted to block data collection/utilization for marketing purposes: "I'd like to deny data sharing for marketing purposes" (#7). One participant limited the use of personal data by using only trusted application: "I'll use only well-known and trusted applications" (#9).

RQ 2: How do users feel about the consent intermediary approach?
During the pre-questionnaire and before the participants were introduced to the concept of a consent intermediary, there was not a clear need for the consent intermediary among the participants, as only 6 participants wanted a way to control where and how their data is shared. However, after the tests 18 participants felt that they need an application similar to our prototype to control data sharing: ”I think it's good to be able to control how data is shared between applications. When I see targeted ads I sometimes think how much data is gathered just based on what I search in Google. In a way it's really scary." (#21) ”I feel like this is how it should be - - *I see this as the natural next step*. The whole smartphone world and all these applications are still such a new thing and now it has just uncontrollably grown to what it is, so this feels like a good tool to tame it." (#18).

One participant was worried about the trustworthiness of the consent intermediary: ”Does the intermediary get authorization from the state?" (#12). A few worried that using an operator might slow down other applications or if the data wasn't compatible with different applications, causing bugs or other problems when using the applications: ”Because of the lack of instructions and information in the application it feels slightly unreliable" (#5) ”I wonder if using the operator slows down my other applications" (#3). Because all of the data sharing is controlled by one application, one participant was afraid that applications could automatically share all data by accident.

RQ 3: How do users feel about a detailed vs simplified (recommendation-based) sharing settings?
After the participants had performed the first task (adding the running app to the intermediary account and sharing the running data to the diary app), they were asked which view they preferred: advanced or recommended (slider). 16 participants preferred the advanced view: it was thought clearer since it provided more information at the first sight compared to recommended view. In addition, the advanced view provided more options to control the data sharing, although a few participants stated that they would likely start using recommended view after understanding how the whole system works. Because all of the participants were new to our concept, it could be argued that the novice users want as much as possible information about the data sharing and consenting options. Only 2 participants preferred the recommended view (#2, #18), mainly because the implementation of the recommended view in our prototype wasn't clear for 11 participants: they didn't understand the purposes because the view didn't provide enough information for novice users. 6 participants did not have a clear preference between advanced and recommended view.

RQ4. How do users feel about a list view vs a more visual presentation of the data sharing connections?
After completing all the tasks, the participants were asked if they preferred the list view or the circular view. 16 participants preferred the circular view mostly because it was easier to see all the connections at one glance: ”It's like a week calendar instead of individual days" (#4), and ”It feels more personal and intuitive" (#7). However, 6

participants preferred the list view because they thought that it was clearer and they liked seeing the icons of the applications: ”It’s easier to see the direction of the data and to process the information in the list view” (#23), ”I can see the icons of the applications and compared to circular view it’s easier to read” (#12).

As a possible improvement, 10 participants suggested drawing a new connection between two services in the circular view as a means of initiating the consenting process for those services.

IV. Discussion

One of the major findings is that before the test the participants had no clear need for a consent intermediary or similar solutions as only 6 out of 23 participants felt they need new tools to e.g. control how their personal data is shared. Yet after the relatively short test 18 participants (~80%) felt that a similar tool would be valuable in controlling their personal data, which shows that people are interested in having better tools to control their personal data and that the consent intermediary approach shows promise.

Participants commented that it would be great if all data sharing is controlled from the same place, but this also raised questions about security: can one’s data be compromised by hacking the consent intermediary account? That depends on the approach chosen by the consent intermediary. If the consent intermediary collects the personal data, as e.g. a personal data store (PDS) does, compromising the intermediary also compromises the data. However, if the intermediary only manages the consents and data flows directly between services, as it does with e.g. MyData, and if the intermediary is designed so that any change to how one’s data is being processed has to be confirmed with one’s trusted device (e.g. a mobile phone), compromising an intermediary account would only reveal what kind on consents one has issued to different services, but no data could be accessed without also compromising the trusted device.

A related question raised by the participants was who is providing the consent intermediary, is it e.g. the government? As the consent intermediary has a key role in controlling how one’s data is processed, the intermediary should be operated by a trustworthy entity. As trustworthiness is a cultural phenomenon, it is natural that in Finland, where government officials, e.g. police, are highly trusted, such suggestion would emerge. However, other countries might prefer solutions that has nothing to do with the government. However, the concept of a consent intermediary leaves much leeway to the implementation and multiple competing intermediaries can emerge from which the individual is free to choose the most suitable for them.

When asked about the alternative ways of showing the linked services and their data flows, 16 out of 23 participants preferred the more graphical view as it e.g. provided a better overview while 6 participants preferred the more traditional list view e.g. due the use of icons to represent the services. The icons could, of course, be used in the more graphical views, which might change the balance somewhat. Further, the need for an overview and the difficulty of using a list-based approach tend to increase as the number of services grows. In the test scenario, there were only 10 services to manage, but in real use even an average individual would easily have dozens if not hundreds of services to manage if they used the consent intermediary to manage all the services that process their personal data. Such a large number of services would likely require even more advanced visualisation to assist in gaining a sufficient understanding of the services and how they share data.

Of the two alternative views for deciding the consenting details, the participants strongly favored the more detailed Advanced view. A possible explanation is that the prototype did not make it clear enough how to view the details behind the slider view or that it was produced by an expert party of the user’s choosing - and the participant felt quite strongly they had to know the details behind the slider to understand it let alone trust it, though a few participants felt they might start using the slider once they got to know the intermediary better. However, this raises an interesting question of scale: if the individual is only provided the detailed view to manage the dozens or hundreds of services they have and the hundreds or even thousands of data connections between the services, this makes the management tedious in the easiest case and impossible in the worse. Better solutions are clearly required, so the slider and similar solutions merit further study. One approach would be to combine the two views so that the individuals sees in real time how the selections in the advance view change when the slider is moved. Such an approach might make the slider approach more useful. Another factor is of course, who has created the slider and how much does the individual trust their recommendations (in the form of the slider). The sliders could be produced e.g. by a suitable consumer/privacy advocate group, but increasingly they could be custom created for the individual by a machine learning based personal privacy assistant.

Major limitations of the study include the sample size: there was only a limited number of participants, most of which were females of similar age and similar background. Yet, the selection was not e.g. technology oriented, so their reactions should in many ways be relative representative of the population at large at least in countries similar to Finland. Another major limitation was that the test took place in a laboratory environment and not with participants real data, which might have made them less careful about sharing 'their' data during the test as there was no risk of their own private health data being leaked to unintended parties. Finally, the amount of services shown in the test was significantly lower than it could be in real life, which might have made the management activities appear easier than they would be in reality.

References

Böhme R and Köpsell S (2010) Trained to accept? A field experiment on consent dialogs. In: *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, Atlanta, USA, 10–15 April, pp.2403–2406. New York: ACM.

Chaudhry A, Crowcroft J, Howard H, Madhavapeddy A, Mortier R, Haddadi H and McAuley D (2015) Personal Data: Thinking Inside the Box. Aarhus Series on Human Centered Computing 1(1).

Cozy Cloud (2018) Cozy cloud website. Available at: https://cozy.io/en/ (accessed 22 November 2018).

Custers B (2016) Click here to consent forever: Expiry dates for informed consent. *Big Data & Society* 3(1).

Digi.me (2018). Digi.me website. Available at: https://digi.me (accessed 22 November 2018).

European Commission (2015) Data Protection. *Special Eurobarometer* (431).

European Union (2016) Regulation (EU) 2016/679 of the European Parliament and of the Council. *Official Journal of the European Union* L119:1–88.

Hub of All Things (2018) Hub of All Things GitHub page. Available at: https://github.com/Hub-of-all-Things (accessed 22 November 2018).

Lehtiniemi, T., & Kortesniemi, Y. (2017). Can the obstacles to privacy self-management be overcome? Exploring the consent intermediary approach. Big Data & Society, 4(2), 1–11.

Meeco (2018) Meeco website. Available at https://meeco.me (accessed 22 November 2018).

de Montjoyeya, Shmueli, E, Wang SS and Pentland AS (2014) openPDS: protecting the privacy of metadata through SafeAnswers. PloS one 9(7).

Poikola A, Kuikkaniemi, K & Honko, H (2015) MyData – A Nordic Model for human-centered personal data management and processing. Finnish Ministry of Transport and Communications.

Solove DJ (2013) Privacy self-management and the consent dilemma. *Harvard Law Review* 126(7):1880–1903.

Turow J, Hennessy M and Draper N (2015) The Tradeoff Fallacy. How Marketers Are Misrepresenting American Consumers And Opening Them Up to Exploitation. *A Report from the Annenberg School for Communication, University of Pennsylvania*.