Opportunities and Challenges of Dynamic Consent in Commercial Big Data Analytics

Eva Schlehahn, Patrick Murmann, Farzaneh Karegar, Simone Fischer-Hübner

Opportunities and Challenges of Dynamic Consent in Commercial Big Data Analytics

Eva Schlehahn[1], Patrick Murmann[2], Farzaneh Karegar[2], and Simone Fischer-Hübner[2]

[1] Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein
[2] Karlstad University

Abstract. In the context of big data analytics, the possibilities and demands of online data services may change rapidly, and with it change scenarios related to the processing of personal data. Such changes may pose challenges with respect to legal requirements such as a transparency and consent, and therefore call for novel methods to address the legal and conceptual issues that arise in its course. We define the concept of 'dynamic consent' as a means to meet the challenge of acquiring consent in a commercial use case that faces change with respect to re-purposing the processing of personal data with the goal to implement new data services. We present a prototypical implementation that facilitates incremental consent forms based on dynamic consent. We report the results gained via two focus groups which we used to evaluate our design, and derive from our findings implications for future directions.

Keywords: Dynamic consent, EU General Data Protection Regulation (GDPR), Human-computer interaction (HCI), Notification, Re-purposing

1 Introduction

Big data analytics can provide organisations with valuable insights. In particular, it may enable companies to understand their customers' preferences and provide these customers with the right information, experiences or services that are of value for them. With big data analytics, new types of data are usually derived that could be utilised for new purposes, which were possibly initially even unforeseen. For protecting privacy and ensuring compliance with the EU General Data Protection Regulation (GDPR), the use of the newly derived data for new data processing purposes could be legitimised by the consent of the individuals concerned (i. e, the data subjects).

Instead of confronting data subjects with long and barely comprehensible consent statements covering all possible future cases of derived data usages at the time when they subscribe to a data service, a more specific consent for the use of newly derived data and/or the processing of data beyond the initially stated data processing purposes could be requested dynamically in the context and at the time when it becomes relevant for the data subject.

Within the scope of the SPECIAL EU H2020 project[3] in cooperation with the Privacy&Us[4] and PAPAYA[5] projects, the concept and management of dynamic consent, which has been initially suggested for the medical domain, has been further refined for commercial use cases.

This paper first discusses the concept and legal motivation for dynamic consent and then presents results of our research in regard to the following research questions:

1. How can user interfaces (UIs) for a commercial use case be implemented to facilitate repurposing via dynamic consent?
2. How is dynamic consent perceived by domain experts?

For addressing these research questions, we have first been developing mock-ups of UIs for managing dynamic consent requests for the re-purposing of TV-viewing profiles for the purpose of targeting customers with event notifications in several iteration cycles. These event notifications concern offline events like concerts, sports, or theatre events that may match the individual interests of the above mentioned customers. These mockups have then been discussed and evaluated in two focus groups with privacy researchers that were held at the IFIP Summer School in August 2019 in Brugg/Switzerland.

The rest of this paper is structured as follows: Section 2 reflects on the requirements pertaining to transparency and consent from the perspective of law and human-computer interaction (HCI), from which we derive a definition of dynamic consent as a means to address the challenges described in a use case related to big data analytics. Section 3 describes the methodology we applied to investigate our research questions by means of designing and evaluating a prototype that implements dynamic consent. Section 4 reports the results we obtained by designing and evaluating our prototype to address our two research questions. In Section 5, we discuss these results and their implications for the design of usable means that facilitate dynamic consent. Section 6 demarcates our contribution from related work, and Section 7 concludes the paper.

2 Background and Motivation

For personal data processing operations based on the legal basis of consent, Art. 6 para. 1 (a) and Art. 4 (11) GDPR, the latter demands a freely-given, informed, unambiguous, and specific indication of a data subject's wish to accept the processing of her personal data by a statement or a clear affirmative action. This individual should be able to clearly understand what data are being collected by what party for what purposes. Moreover, the nature and location of the processing need to be communicated by the controller, as well as with whom which data will be shared [3].

[3] https://www.specialprivacy.eu/
[4] https://privacyus.eu/
[5] https://www.papaya-project.eu/

Recital 32 of the GDPR indicates that electronic means can be used for the request and provision of consent, whereas choosing technical settings for information society services is mentioned as one example. However, especially for complex processing operations, as well as for situations where the use of small mobile screens is involved, this poses a real challenge for data controllers. We address this challenge by a new approach called 'dynamic consent'.

2.1 The concept of dynamic consent

'Broad consent' [9, 14] refers to consent from data subjects for the complete scope anticipated for a particular data processing scenario, including but not limited to, dimensions such as data types, purposes of processing, and additional data. However, such often 'global', long, and jargon-filled consent requests with attached privacy policies usually do not contribute well to a data subject's comprehension about the processing. Rather, they lead to difficulties in comprehension and/or are ignored by users [4,11]. However, for situations of changes to the processing, such as further processing of data beyond the original purpose (re-purposing), controllers lack a communication channel to ask for additional consent. This is all the more complex once special categories of personal data (Art. 9 GDPR) are involved, for which the consent needs to be explicit.

Our dynamic consent approach involves the controller asking the data subject for permission to communicate with them at a later stage after setting up an initial processing operation and requesting the correlating consent for it. Such a permanent communication may be used to facilitate incremental, context-specific consent requests (or at least notifications) addressing changes or intended changes to the original processing operation. These new consent requests are triggered 'dynamically' in the context, whenever the data subject uses other services of the controller.

We define *dynamic consent* as incremental, context-specific consent that will be asked any time after an initial consent was collected. Dynamic consent facilitates the characteristic of being freely-given since it provides granular, context-driven control and a real choice for the data subject instead of having a 'take it or leave it' situation for any complete scope of a data processing scenario. It helps to achieve a specific and unambiguous consent, as the data processing scenarios, especially with respect to data processing purposes, can be defined when they are clear without the demand of generalisation. Dynamic consent facilitates informed consent, as instead of confronting data subjects with all information regarding the data processing scenarios at once, shorter and more specific privacy notices are presented over time, which can help them to afford the time to read and understand what they are requested to agree to.

Service providers, i. e. controllers, can benefit from dynamic consent, as it can legitimise new forms of data processing which go beyond to what the data subjects initially consented to. Moreover, it allows service providers to gradually learn in detail about their users' privacy preferences. Thus, they can adapt their service to meet user expectations, leading to higher satisfaction.

Despite several possible advantages of dynamic consent compared to the traditional consent, dynamic consent may also suffer from a couple of problems. This includes the consent fatigue and habituation, as the number of consent forms users are supposed to handle increases. Hence, we cannot benefit from the ultimate potential of dynamic consent without considering its HCI implications and how users understand and perceive the concept of dynamic consent. Therefore, in this paper, one of our research objectives is to investigate the users' understanding of novel dynamic consent forms designed for a commercial use case.

2.2 Imaginary scenario

The above mentioned dynamic consent approach has been developed within a specific imaginary scenario suitable for mobile devices. The prototype developed has two phases in its UI design, namely the installation of an app, and later notifications handled by this app.

This scenario involves a data subject who already is in a contractual relationship with a data controller for a specific digital service. In this case, this is a digital TV viewing service, for which the data subject at some earlier point in time already has (per assumption for this basic setting) validly consented to the processing of his or her TV viewing behaviour.

The data controller (in our scenario called 'Apricot Ltd.') offers many other digital services, one of them a service which provides recommendations for various events, such as concerts, parties, theatre plays or the like. This service offers the possibility to build a user profile over time in order to give better event recommendations (processing purpose). Depending on what the data subject agrees to, this user profile may consist of data categories such as location of the mobile device the app is installed on, or additional data categories to fine-tune the service to the interests of the user.

These additional data categories could also be information about the data subject's TV-viewing behaviour collected previously. To enable this in a GDPR-compliant way, the data controller needs to ask the data subject for consent to re-purpose this exact information to add it to the event recommendation interest profile.

This imaginary scenario provides a use case that showcases our dynamic consent approach to issues like changes to the processing operation, user comprehension and control, as well as establishing a steady communication channel between controller and data subject.

3 Methodology

3.1 Designing the prototype

Designing the prototype was carried out in multiple iterations. Based on the use case described in Section 2.2, we started by assessing the legal requirements pertaining to the scenario. We complemented them with the informational contents

needed to satisfy these requirements and used both to create initial mockups. The early generations of the designs mainly disregarded aspects related to HCI and principles of usability as regards the future implementation, which necessitated rethinking the design process to accommodate these dimensions.

We therefore started redesigning the prototype in consideration of HCI requirements and discussed each iteration of the design with respect to whether they fulfilled the legal requirements that had been specified earlier. However, the resulting prototypical design, as described in Section 4.1, reflected our own interpretation of how the concept of dynamic consent could be implemented. We therefore decided to seek out independent parties to reflect on the design, which we hoped to accomplish by means of an extended user study.

3.2 Evaluating the prototype

At this early stage of our research, we were mainly interested in receiving feedback related to the conceptual aspects of dynamic consent, which is why we decided to rely on domain experts rather than laypersons to help us evaluate our prototype. To get access to a large variety of privacy researchers and practitioners, we conducted a workshop during the IFIP Summer School 2019, and designed it as a hybrid between a focus group and a cognitive walkthrough. We call it a focus group because its primary purpose was to gauge opinions, feelings and attitudes about the high-level concepts of dynamic consent in the context of re-purposing the processing of personal data in an everyday scenario. Our goal was to obtain as much feedback as possible and therefore encouraged lively discussion among the participants. Additionally, the study exhibited the characteristics of a cognitive walkthrough in that we used a paper prototype to gauge whether the order in which we had designed the operation steps of the prototype helped our test subjects understand the concept we tried to convey. By receiving immediate feedback on individual interaction steps, we tried to ascertain how well the conceptual approach of our design was received.

Participating in our workshop was voluntary. Before beginning the workshop, all participants were informed that no personally identifying information would be collected and that only non-personalised notes would be taken during the group discussions.

We opened the workshop by giving our participants a brief presentation of the use case, including a description of the existing relationship between a data subject and data controller (Section 2.2), and pointed out that during the focus group they would be taking the role of said data subject. We split up the cohort of a total of ten participants into two separate groups. All participants were PhD students at various stages of their studies, and all supplied the domain knowledge of their respective discipline to their group. We distributed the participants evenly among the two groups according to their backgrounds, which covered disciplines such as computer science, information systems, law and psychology, and of which we took note in non-personalised form.

During the first part of the group discussions, each group acted independently, headed by pairs of the four authors who served as moderator and minute-

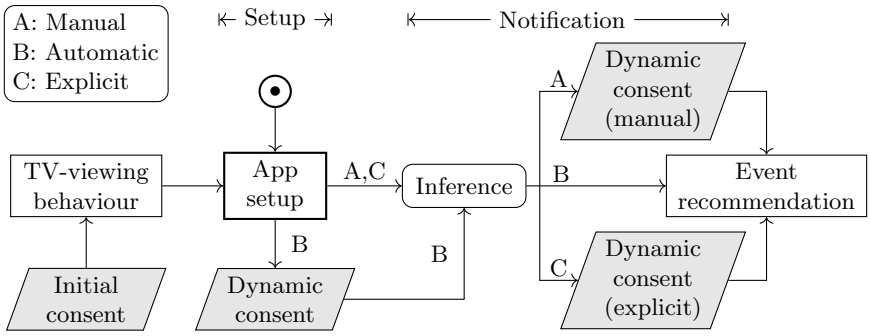


Fig. 1: Schema of improving event recommendations by analysing TV-viewing behaviour. UIs used to collect consent are shaded. Alternative decision paths: A: Dynamic consent based on manual approval, B: dynamic consent based on automatic approval, and C: dynamic consent based on explicit consent.

taker, respectively. At specific stages while going through the prototype, the moderators asked questions from a list we had prepared earlier. Hence, the discussions followed a semi-structured form. The questions helped us to both direct the flow of the discussion and gauge the participants' perception with respect to specific aspects of the scenario. Discussing a list of predefined questions in both groups also helped us achieve consistency for collecting feedback related to our research questions. Each group was equipped with a copy of A3-sheets that represented the screen of the prototype, and stacks of coloured post-it notes they could stick onto the sheets. Additionally, each participant received her own copy of A4-prints that she could refer to at her leisure.

At the end of the workshop, all participants reconvened to compare and discuss the results each group had gathered. We contributed to the discussion by giving our own interpretation of how we thought dynamic consent could help facilitate personal data processing in the context of rapidly developing big data scenarios.

4 Results

4.1 Implementing dynamic consent

Our design is based on the premise of breaking down bulky traditional privacy policies into multiple smaller parts that require less cognitive effort to read and understand. The modular character of dynamic consent would potentially allow for better transparency in that our approach sought to bridge the causal relationship between the change detected in a user's TV-viewing behaviour and the change she would experience thereupon with respect to receiving event recommendations. The approach would enable data subjects to exercise more granular control as regards individual aspects of how their personal data will be processed compared to the extensive scope of traditional consent (Fig. 1).

The use case at hand (Section 2.2) targeted users of mobile devices, which called for a technological artefact in the form of an app running on a mobile phone. We split the prospective run-time behaviour of our app into two distinctive operational phases: a preparatory setup phase and a subsequent notification phase. During the *setup phase*, users of the app, i. e. data subjects, configure the app to reflect their privacy preferences. They do this by specifying to what extent the service provider, i. e. data controller, is permitted to draw from and link multiple sources of the user's personal data to infer from them appropriate candidates for recommending events. We considered three sources of personal data that can potentially be employed to customize event recommendations:

Pre-selected event categories help narrow down the user's interest prior to using the recommendation service. We included this source for the sake of making the prototype appear more authentic. It did, however, not touch upon the concept of re-purposing the processing of personal data.

Location data narrow down the geographical area of events that serve as possible candidates for a recommendation. The use of this data source was tied to a dedicated consent form.

TV-viewing behaviour provides behavioural input as to what kind of events a user might potentially be interested in. This is the data source that the user study focused on.

It was up to users to decide how many data sources they permitted the app to tap into, knowing that a combination of more sources would potentially lead to recommendations that would more adequately reflect their actual interests regarding events.

To provide users with the transparency necessary to understand the causal relationship between their TV-viewing behaviour and the change they would experience with respect to the recommendations they will receive, we relied on a *notification phase* that complemented the setup phase. Delivered via the notification center of the mobile device, notifications were issued in response to changes detected in the user's TV-viewing behaviour, provided these changes impacted the recommendations users would receive at a later time, or in cases when their consent was required to lawfully process their personal data as an effect of the change. These notifications were sent irrespective of any event recommendations a user would receive based on her preferences regarding events.

If users chose to have their TV-viewing behaviour being considered for receiving customised recommendations for events, they were able to select between two modes of operation that determined how they would receive notifications related re-purposing the processing of their personal data (Fig. 2):

Manual (option A). New categories must be acknowledged *manually* as soon as they were detected as a result of a change of the user's TV-viewing behaviour (Fig. 1, Fig. 3 (top), Fig. 4a).

Automatic (option B). Once detected, new categories are added *automatically* without requiring acknowledgement (Fig. 1, Fig. 3 (middle), Fig. 4b).

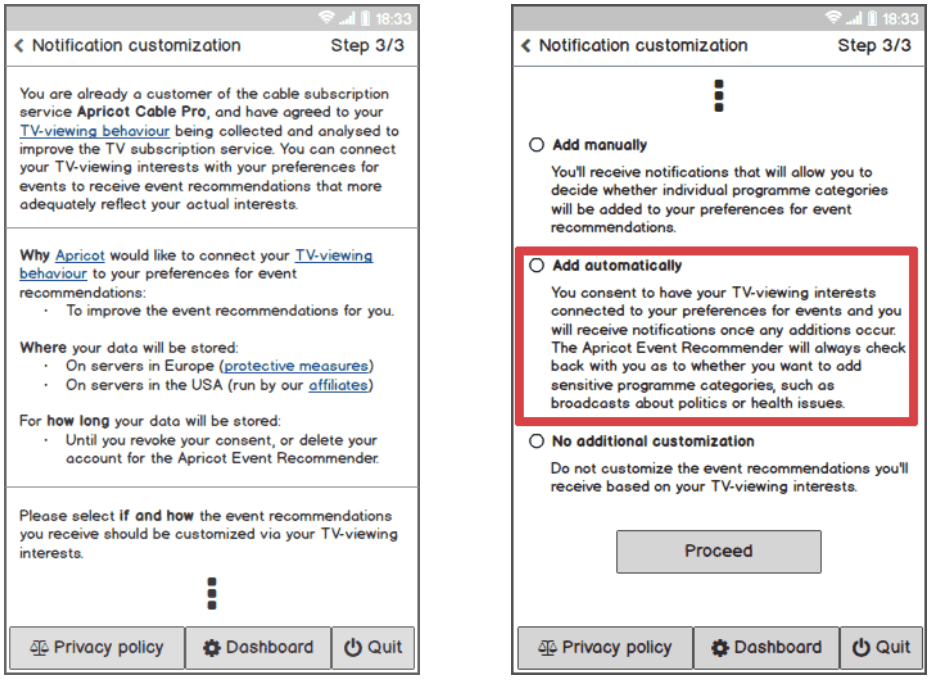
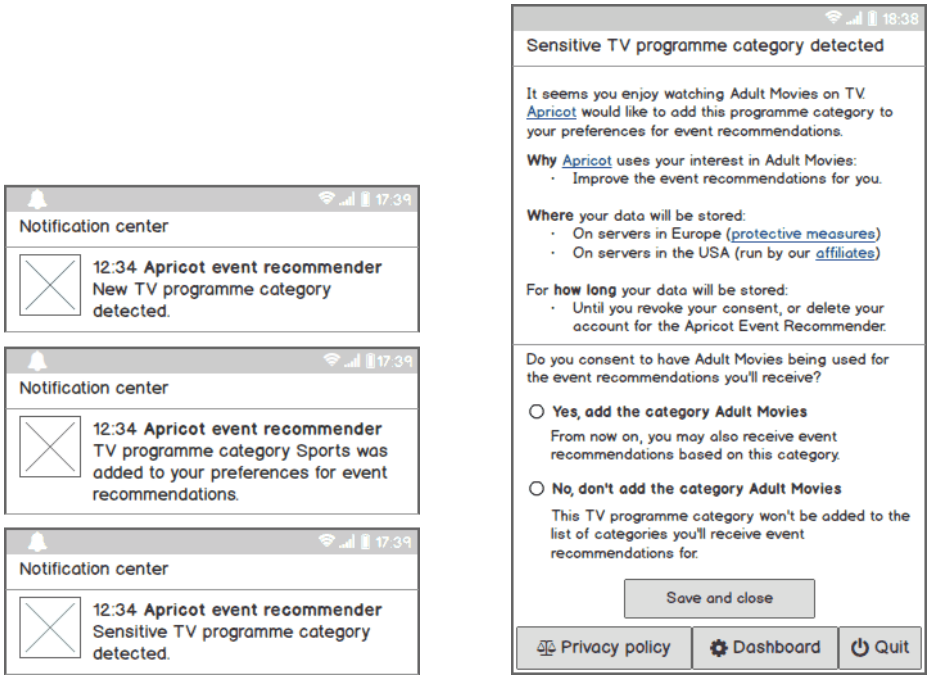


Fig. 2: Setup phase: Choose how TV-viewing behaviour will affect the event recommendations one will receive. Automatic adaptation of the recommendations requires consent *a priori* (framed, highlighting was not part of the original prototype). The screen on the left-hand side continues on the figure to the right.

We conceptualised a third type of notification that would always be issued irrespective of the mode of operation selected previously. It covered cases in which 'special categories of personal data' (GDPR Art. 9) were about to be processed, in which case the data subject's explicit consent would be required (Fig. 1 option C, Fig. 3b). Such cases include, but are not limited to, TV programmes that might allow a data processor to infer the data subject's political opinion or sex life.

We designed the mockup of the app as a click-through prototype. Each of the eleven screens (19 including screens related to stylised secondary information, such as the dashboard or the privacy policy used for collecting initial consent) represented an interaction phase navigable by the user. However, since the purpose of the workshop was to discuss high-level concepts rather than detecting usability issues, we decided to print each screen on paper. That way, we allowed for high accessibility and readability, and ensured that each participant had access to her own copy of the prototype.



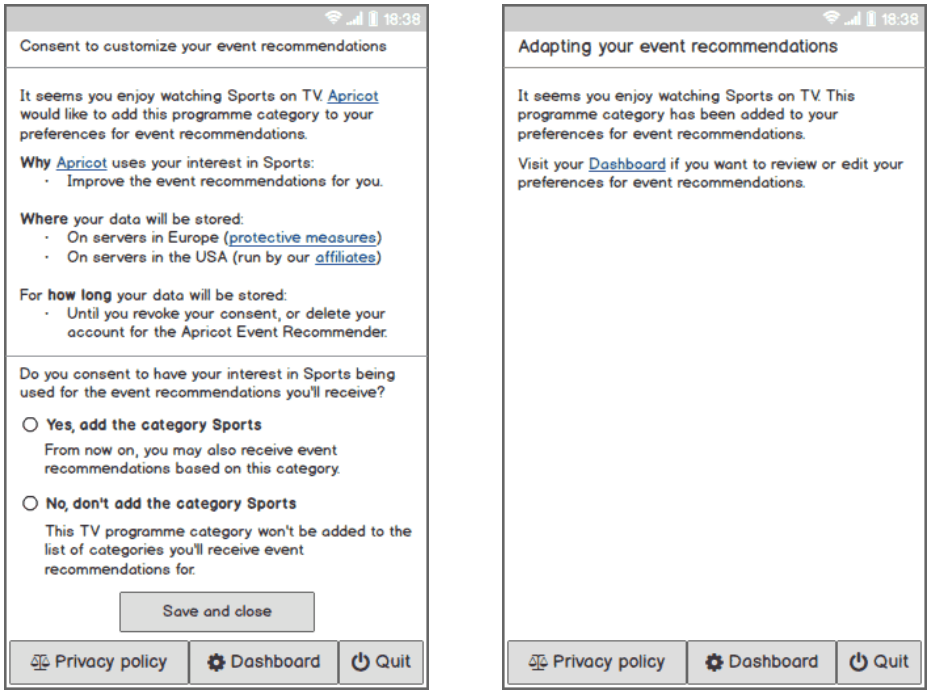
(a) Notification center (b) Sensitive programme category

Fig. 3: (a) Messages delivered via the notification center of the mobile device (A: manual (top), B: automatic (middle), C: sensitive (bottom)), and (b) request of dynamic consent due to the processing of special categories of data (C).

4.2 Perception of dynamic consent

The members of both focus groups were well accustomed to traditional privacy policies, knew how to read them, and were capable of weighing up the pros and cons of individual components of consent forms. When they discussed the consent form related to the processing of location data, e. g., the opinions of individual members varied as regards the completeness and necessity of various aspects, but they all backed up their arguments with a wealth of previous knowledge due to first-hand experience with the subject matter. Most participants appreciated the brief and concise presentation of facts provided throughout the consent forms they discussed. However, some of them requested additional information as regards individual statements made as part of the forms, such as the identity of the data processor outside of Europe.

The concept and usefulness of dynamic consent was perceived differently by the two groups. The members of group 1 seemed capable of conceptually following the scenario as they went through the various stages of the prototype. They understood well that they had earlier consented to the profiling of their TV-



(a) Dynamic consent (manual) (b) Automatic category adaptation

Fig. 4: Notifications received in response to a change of TV-viewing behaviour depending on whether users consented to have their event recommendations adapted automatically.

viewing behaviour when first they had subscribed to the TV-cable service. They realised that the purpose of dynamic consent was to permit the data controller to link that profile to their profile used to customize the event recommendations they would receive. Conversely, group 2 seemed largely unable to follow the train of thought the way in which we had expected them to. They were seemingly unable to see the big picture of the data processing scenario in that they were unable to make a connection between (1) the existing relationship between them, in their role as data subjects, with the data controller as explained in the introductory presentation, (2) their choice to use another online service of the same data controller, and (3) the data controller asking them for additional consent for the purpose of connecting their personal data collected for the first service to their profile that facilitated the second service.

Our participants wanted to stay abreast of any changes detected in their TV-viewing behaviour. When asked to make a choice during the setup phase (Fig. 2), both groups decided to go for manual consent (Fig. 4a, Fig. 1 option A) rather than to rely on automatic consent (Fig. 4b, Fig. 1 option B). Group 1

appreciated the increased level of control they were able to exercise in terms of choosing how they were notified about changes. The members of group 1 noted that in general, dynamic consent is more adapted to the context, as it appears in the context when it is relevant and that it provides good opportunities for mobile phones to provide "step by step policies". By this, users may get "educated" on privacy. However, the members of group 1 also noted that the consequences of the consent could be better clarified in terms of what it implies to be categorised beyond receiving event notifications in the future, e. g. whether further profile details would be added if the user later actually attended a recommended event. They noted that now the question for consent (Fig. 4) is phrased as: "Do you want us to use our profile that we already have for your benefits?" This means that they criticised that consequences were rather stated in terms of utility of receiving customised recommendations than in terms of privacy.

The members of group 1 remarked that they would have liked even more control in terms of exercising intervenability, such as having access to shortcuts in the form of buttons that would allow them to revoke their consent by means of the notification itself. This would save them time and effort compared to invoking the dashboard, searching for the required option in question, and then making the change. Both groups noted that the dashboard should be more visible, and that further instructions would be required on how transparency and intervenability rights can be exercised.

Group 1 members discussed the dynamic explicit consent requests for sensitive TV-programme categories (Fig. 3). It was noted that these explicit consent requests can be embarrassing and compromising, e. g. if they appear when someone is together with her partner or a colleague, or at any other unexpected occasion when others can watch this consent request. Hence, dynamic consent requests for sensitive categories should not appear directly, which emphasises the need for a 'notification center', as we have implemented in our mockups (Fig. 3a (bottom)).

Conversely, group 2 seemed confused by the repetitive nature of the follow-up consent forms, which they had to go through as part of receiving notifications about changes related to their TV-viewing behaviour. They were unable to relate the consent forms to choices they had made earlier during the setup phase and perceived them as redundant and tedious.

5 Discussion

5.1 Reflecting on dynamic consent

Sections 2 and 6 motivate dynamic consent as regards its characteristics of being specific, freely given and informed, compared to traditional consent. Despite the fact that dynamic consent can help break down a comprehensive, anticipatory consent form into the parts that are actually applicable to the data processing scenario in question, dynamic consent will not, in itself, solve the inherent issue of readability and intelligibility. Privacy notifications will still have to be designed such that they cater towards the specific needs of the individual reading

the contents, that they clearly communicate risks and consequences in terms of privacy that will or may arise due to acting and not acting in response to the notification, and that they provide support and guidance in case recipients are unable to make an informed decision solely based on the information currently at her disposal [12]. In this respect, dynamic consent can not mitigate the effect of a consent form that was designed poorly in relation to its content or structure.

Clarity will be indispensable in cases when the circumstances under which a notification has been issued are delicate and when particular care is required. This will, e. g., be the case when notifications report about or ask consent for the processing of sensitive personal data (GDPR Art. 9). Multilayered policies could be a key enabler as regards providing a customisable depth of information for dynamic consent [3, 12]. By doing so, the cognitive load imposed upon readers of information provided on the highest layer would be comparatively low, while lower layers would still allow for more detailed information upon request. As was requested by some of our participants, such information could, e. g., elaborate on specific statements made in the consent form, or on the exact consequences that will arise for a data subject should she choose to link a particular TV-programme category to the profile used for sending her event recommendations.

In our study, we did not attempt to cover the longitudinal aspect introduced by the asynchronous nature of notifications as such. Notifications may not only arrive at inopportune moments, as discussed by focus group 1, but also at times when a data subject may not immediately be able to comprehend the causal relationship between a message and the cause that has triggered it [16]. Despite the fact that informational content conveyed as part of the notification may in itself be more comprehensible compared to traditional consent forms, assessing the causal relationship of temporally asynchronous events may impose additional cognitive load on recipients of notifications. Privacy notifications will therefore have to implement appropriate contextual cues to support users in understanding the contextual relationship reported by the notification [12].

Some of our participants requested additional means of intervenability from within the notifications themselves. This is in line with previous findings in the literature in that privacy notifications should provide actionable choices in addition to the informational content provided in the message [6]. It corresponds to the legal requirement stipulated in GDPR Art. 7 (3) and the recommendations of the Art. 29 Working Party [1] in that consent should be as easily revocable by data subjects, as it was given. Hence, designers of future prototypes should consider adding actionable choices to notifications, which would help data subjects exercise specific data subject rights according to the situation at hand [12].

More research will be required to investigate the longitudinal aspect of dynamic consent as regards user perception. Authentic results may be obtained via studies in which users of a data service make decisions that affect the processing of their actual personal data, and in which they provide situational feedback on the perceived utility of dynamic consent as part of the process.

5.2 Limits

As is pointed out in Section 3.2, we specifically targeted domain experts for the initial evaluation of our prototype. The participants of our focus groups were not only highly educated, but also comparatively young. Our findings can therefore not be generalised for the general public. Older, less knowledgeable users or users who are less familiar with employing mobile devices in the context of IT might not exhibit the same level of expertise as regards the socio-technological ecosystem reflected in our study. For such an audience it might be even more difficult to fully comprehend the longitudinal process accompanying the concept of dynamic consent, and might therefore be unable to make informed decisions as regards the processing of their personal data.

The contents reflected in the focus groups were relatively broad and required considerable time to process by our participants. In particular, many of the screens and UIs discussed during the focus groups were not strictly related to the concept of dynamic consent. We had included some of the screens primarily for the sake of authenticity, i. e. to make our prototype and the underlying use case more tangible. Future studies would be well advised to focus on the aspects that are essential for conveying the concept of dynamic consent, namely the consent form by which users choose how they will be informed about future changes (Fig. 2), and the notifications used to facilitate the subsequent consent management (Fig. 3, Fig. 4).

Similarly, some of the dimensions considered during the study did not contribute to convey the concept of dynamic consent as such. Location data, e. g., were not relevant for discussing repurposing TV-viewing behaviour to facilitate event recommendations. If such marginalia were removed, the study would focus even more on the actual core concept of the subject matter.

6 Related Work

Privacy nutrition labels [10], multi-layered short policies summarising key data practices [2, 3], privacy icons and images [5, 7], and comic-based interfaces to convey policy information [17] are examples of proposed solutions to solve the issues of traditional consent forms discussed in Section 2. Nonetheless, none of the methods proposed could adequately address the consent problems in various contexts. This motivated researchers to propose other solutions for achieving consent, such as Just-In-Time Click-Through Agreements (JITCTAs) [13] and dynamic consent.

The concept of JITCTA proposed by Patrick and Kenny [13] is based on subdividing a "large, complete list of service terms" [13] into smaller 'agreements' that collect consent from data subjects as needed, i. e. once conditions apply that require personal data to be processed in a specific way. Kay and Terry [8] interpret JITCTAs as segmenting a larger legal agreement into smaller parts that are presented at situationally appropriate times. Both groups of authors argue that by confronting users with small pieces of context-sensitive information compared

to a large amount of anticipatory information, the cognitive load necessary to process such information can be reduced, while the level of specificity increases.

Conversely, dynamic consent as we consider it in this paper does not rely on the largest possible superset of a privacy policy defined *a priori*, which is dealt out in smaller portions once the need arises. We instead assume that the necessity to process personal data changes over time, potentially in a way that could not have been foreseen when the preceding version of the policy was issued. Due to the causal relationship between observed user behaviour and change of how data are processed, however, we share with these authors the opinion as regards an increase in specificity and, potentially, an increased level of understanding on the part of users of such data services.

Dealing with multiple researchers and projects in biobank research makes it difficult to obtain informed consent from participants for all future uses of data at the time of recruitment into the biobank [9]. Kaye et al. [9] argue that re-consenting, to overcome the issues of informed consent in the biobank research is costly and time-consuming in practice and might lead to high drop-out rates due to the difficulty in locating people. A practical solution, as discussed in [9, 14], to open-ended projects in biobank research is broad consent. However, using the broad consent model may not help to achieve informed consent [9, 14].

An alternative solution for consent in biobanks in some form of a dynamic consent approach was initiated for the first time in the EnCoRe project[6] (June 2008 to April 2012). In this solution, collecting consent for three biobanks was supposed to be replaced with broad consent [9]. Researchers elaborated on the pros and cons of dynamic consent in biobanks [9,15] and discussed the implementation issues of the dynamic consent model in practice [9]. Although dynamic consent is participant-centred, allows interactions over time, and protects participants' autonomy over their data [9, 14], it requires, above all of the physical resources, a commitment to such a vision by stakeholders involved in the biobank research such as clinicians and researchers, health-care services, and governments for its deployment in real scenarios [9].

Kaye et al. [9] argue that while dynamic consent is proposed as a concept related to a biobank project, it is an approach that can be applied more broadly in other fields beyond healthcare. To apply dynamic consent in other contexts, we require more research regarding its applicability to solve the issues of current traditional consent forms. Hence, we redefined the concept of dynamic consent for online service providers, specifically for commercial data services using big data analytics based on their users' consent. Nonetheless, there are some differences in practice between the dynamic consent in biobank research and the dynamic consent we defined in this paper. For the former, the data collected, processed, and re-purposed are always special categories of data; thus requiring explicit consent by law. For the latter, on the contrary, there are different levels of sensitivity for the data being processed which relieves the data controller of the need to always obtain explicit consent. It introduces more opportunities for implementing dynamic consent, which can potentially fulfil different users'

[6] `http://www.encore-project.info/`

requirements. However, it comes with its own challenges as how to facilitate consent in cases when dynamic consents is not requested explicitly (see Fig. 1 option A and Fig. 1 option B). This calls for more investigation on the effects of dynamic consent on users' experience, their understanding of their data flow and conditions of consent, and their sense of oversight and control.

7 Conclusion

This paper presents a novel approach for obtaining dynamic consent for a commercial scenario, which was evaluated by expert focus groups at the IFIP Summer School 2019. Our expert evaluations showed that our approach involving alternative paths for obtaining dynamic consent was not easily understood by all experts. Nevertheless, those that understood how the concept of dynamic consent was used in our scenario also appreciated the approach of incremental consent requests. These can more specifically describe the current context and provide increased user control and transparency. However, at the same time, emphasis must also be put on informing users well about privacy consequences when choices need to be made. This dynamic way of collecting or altering the data subject's permissions over time should come along with meaningful ways to exercise intervenability, including the data subject's rights entailed in the GDPR. This in particular needs to provide the user with direct access to functions for easily revoking a previously given consent at the moment when a request to dynamically extend this consent appears. Future directions for the design of dynamic consent should address these results of our expert evaluations.

Acknowledgements

The research presented in this paper was jointly conduced by the SPECIAL, Privacy&Us and PAPAYA EU projects. The project SPECIAL (Scalable Policy-awarE linked data arChitecture for prIvacy, trAnsparency and compLiance) has received funding from the EU's Horizon 2020 research and innovation programme under grant agreement No. 731601. The Privacy&Us project has been supported by the EU's Horizon 2020 Research and Innovation Programme under the Marie Skłodowska-Curie Grant 675730 and the project PAPAYA (A Platform for Privacy Preserving Data Analytics) is funded by the H2020 Framework of the European Commission under grant agreement No. 786767.

We thank Harald Zwingelberg (ULD) and Rigo Wenning (ERCIM/W3C) for their valuable insight, ideas and contributions to the concept of dynamic consent, and also the participants of the two focus groups for their valuable feedback.

References

1. Art. 29 Data Protection Working Party: Guidelines on consent under regulation 2019/679 (2018)

2. Art. 29 Data Protection Working Party: Opinion 10/2014 on more harmonised information provisions (Adopted on 25 November 2004)
3. Art. 29 Data Protection Working Party: Guidelines on transparency under Regulation 2016/679 (Revised and Adopted on 11 April 2018)
4. Cate, F.H.: The Limits of Notice and Choice. IEEE Security & Privacy **8**(2), 59–62 (2010)
5. Cranor, L.F., Guduru, P., Arjula, M.: User interfaces for privacy agents. ACM TOCHI **13**(2), 135–178 (2006)
6. Egelman, S., Cranor, L.F., Hong, J.: You've Been Warned: An Empirical Study of the Effectiveness of Web Browser Phishing Warnings. In: Proc. SIGCHI Conference on Human Factors in Computing Systems. pp. 1065–1074. ACM (2008)
7. Holtz, L.E., Zwingelberg, H., Hansen, M.: Privacy policy icons. In: Privacy and Identity Management for Life. pp. 279–285. Springer (2011)
8. Kay, M., Terry, M.: Textured agreements: Re-envisioning electronic consent. In: Proc. Sixth Symposium on Usable Privacy and Security. p. 13. ACM (2010)
9. Kaye, J., Whitley, E.A., Lund, D., Morrison, M., Teare, H., Melham, K.: Dynamic consent: a patient interface for twenty-first century research networks. European Journal of Human Genetics **23**(2), 141 (2015)
10. Kelley, P.G., Cesca, L., Bresee, J., Cranor, L.F.: Standardizing privacy notices: An online study of the nutrition label approach. In: Proc. CHI. pp. 1573–1582. ACM (2010)
11. Luger, E., Moran, S., Rodden, T.: Consent for all: Revealing the hidden complexity of terms and conditions. In: Proc. CHI. pp. 2687–2696. ACM (2013)
12. Murmann, P.: Eliciting Design Guidelines for Privacy Notifications in mHealth Environments. International Journal of Mobile HCI **11**(4), 66–83 (2019)
13. Patrick, A.S., Kenny, S.: From Privacy Legislation to Interface Design: Implementing Information Privacy in Human-Computer Interactions. In: International Workshop on Privacy Enhancing Technologies. pp. 107–124. Springer (2003)
14. Ploug, T., Holm, S.: Meta consent: A flexible and autonomous way of obtaining informed consent for secondary research. Bmj **350**, h2146 (2015)
15. Prictor, M., Teare, H.J., Kaye, J.: Equitable participation in biobanks: The risks and benefits of a "dynamic consent" approach. Frontiers in public health **6** (2018)
16. Schaub, F., Balebako, R., Cranor, L.F.: Designing Effective Privacy Notices and Controls. IEEE Internet Computing **21**(3), 70–77 (2017)
17. Tabassum, M., Alqhatani, A., Aldossari, M., Richter Lipford, H.: Increasing user attention with a comic-based policy. In: Proc. CHI. pp. 200:1–200:6. ACM (2018)