Olha Drozd and Rigo Wenning and Sabrina Kirrane

Enabling Personal Data Processing Control via Dynamic Consent

Conference or Workshop Item (Accepted for Publication)
(Refereed)

Enabling Personal Data Processing Control via Dynamic Consent

Olha Drozd[1], Rigo Wenning[3] and Sabrina Kirrane[1]
[1]Vienna University of Economics and Business, Austria
[3]W3C, Sophia-Antipolis, France

In the General Data Protection Regulation (GDPR) the processing of personal data is prohibited via Art. 6 except for some predefined scenarios (e.g.: public interest (GDPR art. 6(1)(e)), legal obligations (GDPR art. 6(1)(c))) and when the data subject has consented (GDPR art. 6(1)(a)) to his or her personal data processing. According to the GDPR, **consent requests** shall specify clearly which *data* is processed, what is the *purpose* of the processing, what *processing* will be performed, where and for how long the data is *stored*, and whether or not the data will be *shared* with others. Currently, the way to obtain consent is to have a human readable description of the data processing where the processing is described in some very general terms. Such multipage documents detailing all eventual data collection done by the entire service are there for legal purposes and not for the user. In such cases, the user doesn't know whether a certain data item was collected or not, and what usage constraints (if any) are attached to it. Such consent is neither specific nor informed.

Existing, research points to the cognitive limitation of users when it comes to informed consent [1, 2, 4]. One approach, which could potentially overcome such cognitive limitations is the use of **dynamic consent** instead of a ready-made, set in stone, static consent forms. Dynamic consent is a relatively new framework, arising from work in the biomedical domain, that refers to the use of modern communication mediums to provide transparency, enable consent management and to elicit greater involvement of data subjects from a consent perspective [3].

In this demo, we present the first version of our **dynamic consent and control user interface** (UI), which is tailored to the following exemplifying use case scenario:

> *Sue, a business administration student, buys a wearable appliance for fitness tracking from BeFit. She is presented with a dynamic informed consent request, comprised of a data usage policy that describes which data shall be collected, why they are collected, how they will be processed, stored and shared in order to give her fitness-related information.*

Since we want to involve real data subjects at the early stage of the UI design, we developed a fully functional online version[1] of our first consent request, where we followed Jackob Nielsen's usability heuristics for user interface design[2]. Our dynamic consent request provides the following functionalities:

Categorization. We grouped information according to five categories, namely purpose, data, storage, sharing and processing. This grouping is realized in the form of tabs with a name and an icon for each category.

Customization. The user can adjust their consent specifically to their wishes. There is also a possibility to drill down a concrete path and agree only to that path. For example, users can allow BeFit to process their resting heart rate (*data*) to be displayed to them in BeFit's app (*purpose*) by performing on-device calculations (*processing*) and saving the data on their device (*storage*) without sharing it with anybody.

Revocation. In our use case the consent is given for the first time before using the device and the consent withdrawal in our interactive UI wireframe is tailored to this use case.

Understandability. To increase the understandability of the consent request we are using plain language and standard icons. Our dynamic consent request is also supported by a graph that shows every possible unique path for selected items.

In the course of our research we are going to develop multiple versions of the UI wireframes for the dynamic consent request backed by the user study results.

REFERENCES

[1] A. Acquisti, I. Adjerid, and L. Brandimarte. Gone in 15 seconds: The limits of privacy transparency and control. IEEE Security & Privacy, 11(4):72–74, 2013.
[2] F. Z. Borgesius. Informed consent: We can do better to defend privacy. IEEE Security & Privacy, 13(2):103–107, 2015.
[3] I. Budin-Ljøsne, H. J. Teare, J. Kaye, S. Beck, H. B. Bentzen, L. Caenazzo, C. Collett, F. DâAZAbramo, H. Felzmann, T. Finlay, et al. Dynamic consent: a potential solution to some of the challenges of modern biomedical research. BMC medical ethics, 18(1):4, 2017.
[4] A. M. McDonald and L. F. Cranor. The cost of reading privacy policies. ISJLP, 4:543, 2008. URL http://heinonline.org/hol-cgi-bin/get_pdf.cgi?handle=hein.journals/isjlpsoc4&section=27.

[1] https://cr-wizard-en.firebaseapp.com/wizard

[2] https://www.nngroup.com/articles/ten-usability-heuristics/