Using the Consent Request User Interface Prototype

Olha Drozd[0000−0001−6551−6567] and Sabrina Kirrane[0000−0002−6955−7718]

Vienna University of Economics and Business, Vienna, Austria
{olha.drozd, sabrina.kirrane}@wu.ac.at

An IFIP SELECT paper for IT professionals based on the research paper:
Drozd O., Kirrane S. (2020) Privacy CURE: Consent Comprehension Made Easy. In: Hölbl M., Rannenberg K., Welzer T. (eds) ICT Systems Security and Privacy Protection. SEC 2020. IFIP Advances in Information and Communication Technology, vol 580. Springer, Cham.

1 Relevance to Information Technology Professionals

Data privacy laws and guidelines vary significantly with each jurisdiction around the globe and even within economic sectors. Also, the ability for users of a software application to understand what they are consenting to depends on how well the relevant data privacy options are communicated to the user via that application's user interface. The resulting lack of consistency created by these two realities causes confusion for everyone concerned. This research paper proposes a prototype solution to this problem; a Consent Request User Interface (CURE) that enables a user to confidently determine how to select privacy settings that he or she needs.

In the United States (US), the Federal Trade Commission's fair information practice principles (FIPPs), that serve as a framework for various state and federal laws in the US concerning privacy in different economic sectors (e.g., governmental, financial, healthcare) [4], and also the California Consumer Privacy Act (CCPA), recommend or require, in some predefined scenarios, obtaining consent from data subjects for the processing of their personal data. The second FIPPs principle, entitled *choice/consent*, states that data subjects should be able to control how personal information collected from them is processed when it comes to secondary processing. Privacy laws in the US predominantly make use of opt-out consent, where the data processing happens unless data subjects withdraw their consent. However, opt-in consent is also required in some specific cases, for instance the CCPA prohibits businesses from selling personal information relating to consumers who are between 13 and 16 years old without their consent.

In the European Union (EU), the General Data Protection Regulation (GDPR) lists[1] consent as one of the six legal bases for the personal data processing to be lawful. The GDPR defines the notion of consent in Article 4(11): *"consent of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies*

[1] GDPR Art. 6

agreement to the processing of personal data relating to him or her". Even though the GDPR[2] and guidelines on consent under Regulation 2016/679[3] from Article 29 Working Party[4] provide clear requirements for consent to be lawful, inspections by data protection authorities in different EU countries show that the current technical solutions for acquiring consent in relation to cookies on various websites do not comply with GDPR. Thus, data protection authorities impose fines[5] on the companies that breach GDPR. For instance, the Spanish data protection authority fined[6] IKEA for displaying a cookie consent banner on their website that was not GDPR compliant because it did not provide enough information about data processing for the consent to be informed, there was no clear rejection mechanism, and the cookies were placed on users' computers prior to obtaining consent. Additionally, some services still use static general descriptions of current and future data processing; however, these are not specific, hard to digest [6], and do not constitute informed consent.

Despite some attempts to give users more control and transparency regarding personal data processing [3,5], the cognitive limitation of data subjects, in terms of understanding what exactly they consented to, also remains an open research challenge [1,2]. In order to address the GDPR compliance and consent comprehension challenges, in our research paper, we present a consent request user interface prototype, which provides transparency regarding personal data processing, more control via customization, and improves users' comprehension with respect to what they actually consent to.

2 CURE Prototype Utility

Figure 1 depicts the CURE prototype - a web application consent request developed for laptops and desktop computers. The prototype is split into two components: slider (see Figure 1 (1)) and consent per purpose (see Figure 1 (2)). The main features of the CURE prototype are: (i) categorization of purposes; (ii) granular consent customization; (iii) improved understandability; and (iv) easy consent revocation.

The GDPR and the Article 29 Working Party guidelines on consent under Regulation 2016/6791 served as a source for the prototype requirements. Even though the requirements were derived from the GDPR, the results of our research could potentially be used in other jurisdictions. Although we based our prototype on an exemplifying use case scenario concerning consent requests for wearable appliances for fitness tracking, our prototype could be applied in different contexts.

The CURE prototype was assessed with the help of a usability evaluation. The prototype was well received by the participants and performed better in comparison with the classical consent requests in the form of privacy policies as well as with the solution offered by Usercentrics[7] that describes itself as *"the market leader in the*

[2] GDPR Art. 4(11), Art. 6, Art. 7, Recitals 32, 33, 42, 43

[3] Guidelines on consent under Regulation 2016/679. https://bit.ly/2BdQs08

[4] Article 29 Working Party was an independent European working party that dealt with data protection issues. On 25.05.2018 it was replaced by the European Data Protection Board under the GDPR.

[5] GDPR Art. 83

[6] Resolution of sanctioning procedure. https://www.aepd.es/es/documento/ps-00127-2019.pdf

[7] Usercentrics. https://usercentrics.com/

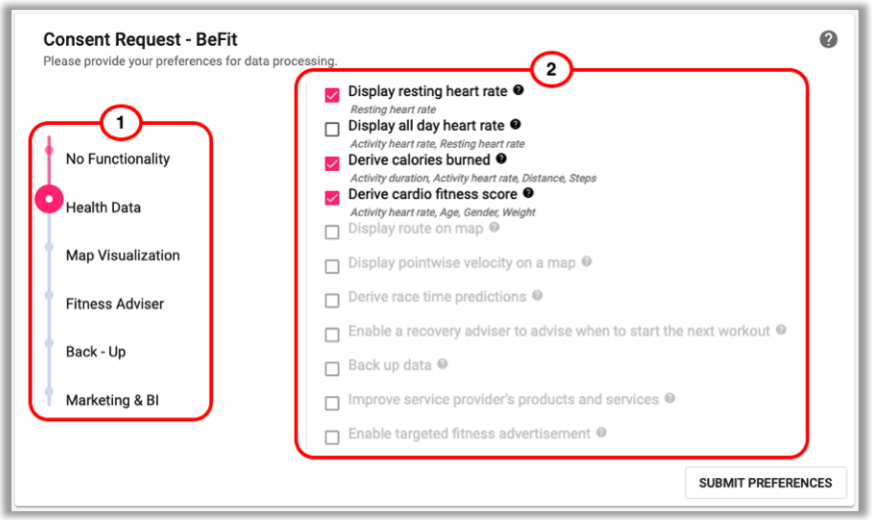

Fig. 1: The CURE prototype: (1) Slider. (2) Consent per purpose.

area of enterprise consent management platforms". Based on the video recordings, the participants performed all tasks quickly, easily, and almost without errors. They typically spent one second on each evaluation task relating to the giving or withdrawing of consent. They described the prototype mostly with positive adjectives (e.g., easy to use, useful, clear, helpful, usable, effective). The overall comprehension of the users' consent was very high. On average, 86% of the participants remembered all the data processing information that they consented to.

The fully functional prototype[8], its source code[9], as well as the questionnaire[10], used in the evaluation, are available online. Additionally, the proposed evaluation material could serve as the basis for a consent benchmark.

In terms of impact, our work follows the GDPR requirements and improves data subjects' comprehension with respect to the processing and sharing of their personal data and what exactly they have consented to, as opposed to the current situation, where each application has a different consent request design and formulation approach causing information overload from a user perspective.

References

1. Acquisti, A., Adjerid, I., Brandimarte, L.: Gone in 15 seconds: The limits of privacy transparency and control. IEEE Security & Privacy **11**(4), 72–74 (2013)
2. Borgesius, F.Z.: Informed consent: We can do better to defend privacy. IEEE Security & Privacy **13**(2), 103–107 (2015)

[8] The prototype is available in two languages: English (http://cr-slider.soft.cafe/en/) and German (http://cr-slider.soft.cafe/de/).
[9] The source code is available at https://bit.ly/2GErFC7.
[10] The questionnaire is available at https://bit.ly/2DNOGC3.

3. Costante, E., Sun, Y., Petković, M., den Hartog, J.: A machine learning solution to assess privacy policy completeness:(short paper). In: Proceedings of the 2012 ACM workshop on Privacy in the electronic society. pp. 91–96. ACM (2012)
4. Hughes, P.P., Goldstein, M.M.: Privacy, Security, and Regulatory Considerations as Related to Behavioral Health Information Technology, chap. 16, pp. 224–238. Oxford University Press, Oxford (2016)
5. Kelley, P.G., Bresee, J., Cranor, L.F., Reeder, R.W.: A nutrition label for privacy. In: Proceedings of the 5th Symposium on Usable Privacy and Security. p. 4. ACM (2009)
6. McDonald, A.M., Cranor, L.F.: The cost of reading privacy policies. ISJLP **4** (2008)