Zaira Zihlmann, Kimberly Garcia, Simon Mayer, and Aurelia Tamò-Larrieux (2022): A right to repair privacy-invasive services: Is a new, more holistic European approach emerging? In: Proceedings of the International Conference on Privacy-friendly and Trustworthy Technology for Society – COST Action CA19121 - Network on Privacy-Aware Audio- and Video-Based Applications for Active and Assisted Living

A right to repair privacy-invasive services: Is a new, more holistic European approach emerging?

Zaira Zihlmann[1], Kimberly Garcia[2], Simon Mayer[2], and Aurelia Tamò-Larrieux[3]
[1] University of Lucerne, Lucerne, Switzerland
[2] University of St. Gallen, St. Gallen, Switzerland
[3] Maastricht University, Maastricht, The Netherlands
zaira.zihlmann@unilu.ch; kimberly.garcia@unisg.ch; simon.mayer@unisg.ch; a.tamo@maastrichtuniversity.nl

Abstract

The terms of use of online services are often constructed as binary options which leads to take-it-or-leave-it decisions by users: either one agrees to the data processing practices of the service provider and gets access to the service, or one does not agree and cannot use the service. Research shows that consent notices do not provide actual control to users over how their data is being processed due to numerous reasons, such as not reading policies (Custers et al., 2018), privacy fatigue (Choi, Park and Jung, 2018), and manipulative designs (Waldman, 2020). Against this backdrop we conceptualized a right to customization that should provide users with the right to demand that virtual services are customized in a manner that reflects their privacy needs (Tamò-Larrieux et al., 2021). Our concept

roots in the GDPR, specifically on the right to data portability (Article 20) and on the principle of data protection by design and default (DPbDD) enshrined in Article 25. We argue that DPbDD enables data subjects to demand technical and organizational measures to be put in place and that operalizing DPbDD requires thinking about the whole life cycle of data, individual rights, the ideas of individual participation and control aspects. Furthermore, we use the right to repair as a source of inspiration. Calls to update the right to repair to include obsolete software have been raised and recently the CJEU *de facto* recognized a right to repair for software in the case Top System SA v Belgian State[1] (van Holst, 2021). This fundamentally changes the scope of repair and should according to our analysis be broadened even more to include modifications of software-based services for better privacy protection.

From a technical perspective the key question becomes how to empower individuals with respect to their data. The right to customization could be achieved through two technological approaches, namely service variants and service alternatives. In the former, a Data Controller (DC) creates and actively curates a catalog of software variants that collect and use different types of user data to provide the same (or very similar) functionality. Thus, users can opt for highly personalized experiences or just the service core functionality. In the latter approach, the DC provides interoperable and interchangeable service alternatives allowing users to retain control of their data by granting fine-grained access to it (e.g., through Solid, the Social Linked Data project[2]). In practice, this would mean that e.g., users of a voice assistant could, based on the right to customization, require the DC to apply certain restrictions to the service, such as restricting the recording of voices at a certain time of day or removing recordings of children's voices before cloud uploads. In this scenario, the DC would either have to create a variant that implements the users' customization requests or allow the use of another service that makes these customizations before uploading the data.

We see further technical developments heading in the same direction as we do with our proposal towards considering service variants and alternatives. For instance, the Smart Speaker Blocker (Olade et al., 2020) is an intermediary device that aims to intelligently filter out sensitive conversations and thus prevents this information from reaching a microphone in the first place. Users should even have the possibility to completely hide all identifying information by allowing the smart speaker only to receive a synthesized text-to-speech voice. Instead, Cheng et al. (2019) aim to provide users with control over the recording behavior of voice assistants. They propose that a user could employ a tagging device that emits an acoustic signal and signals the system that the user does at the moment not consent to recording. Another technology development that shows the feasibility of creating

[1] CJEU judgment of 6 October 2021, Top System SA v Belgian State, case C-13/20, EU:C:2021:811.

[2] https://solidproject.org/

service variants is Apple's App Clips for iOS[3]. App Clips are a small part of an app that provide a specific functionality. Thus, users do not need to install software that they might never use, or sign up for accounts that might be only used once. Tracking data is limited in App Clips and they are automatically removed from a device 30 days after they are used.

With respect to service alternatives, we see first implementations for instance by the Flemish government that is currently testing Solid for public services via the "My Citizen" profile. The profile brings together data from different parts of the administration into a single, easily accessible application. Through their profile, citizens can then access a personal overview of government services and can navigate to the respective service. This furthermore allows citizens to share personal information with government entities while their data remains within the personal data store (CDEI, 2021).

While the technical tools described above and the Flemish project show that it is technically and politically feasible to give more control to users, there are also some limitations: From the user's perspective, exercising the right to customization requires a deeper understanding of the system which can have a negative impact on the ease of use. To tackle this issue, we envision "customization communities", analogous to the emergence of so-called Repair Cafés that facilitate exercising the right to repair. Furthermore, the role of intermediary services such as Solid, needs to be further analyzed and qualified in order to identify the potential risks and challenges they encounter (e.g., their responsibility in case there is a data breach in the Pod). This aspect is related to the absence of a legal framework that comprehensively underpins and guides these technological efforts.

However, developments in this direction are emerging in the EU as we see new regulations that push towards the empowerment of individuals with respect to their data. In its communication "A European strategy for data", the EU Commission states that "[i]ndividuals should be further supported in enforcing their rights with regard to the use of the data they generate. They can be empowered to be in control of their data through tools and means to *decide at a granular level* about what is done with their data ('personal data spaces')" (European Commission, 2020, p. 20, emphasis added). According to the Commission, this could be achieved by strengthening the right to data portability, e.g., by imposing stricter requirements on interfaces for real-time data access and the mandatory use of machine-readable formats for data from certain products and services, such as data from smart home devices. Beyond that, rules for new types of data intermediaries such as providers of 'personal data spaces' might be considered. The Commission is aware of technical tools such as Solid that enable users to decide at a granular level what happens to their data, and it recognizes the great potential of these tools as well as the need for a supportive environment for them (European Commission, 2020).

---

[3] https://developer.apple.com/app-clips/

Legislative action in this respect is underway. First, we can observe that the proposal for a Regulation on Privacy and Electronic Communications[4] points to the initially described issues of consent and states that users should have the possibility to grant consent through software settings and providers of software are encouraged to include settings in their software which allows end-users to manage consent (Recital 20a). Heading in the same direction, the recently proposed Data Act[5] aims to empower individuals with respect to their data as well as to enhance innovation and competition among EU businesses. It inter alia foresees provisions that should permit users of connected devices to access the data they generate and to share it with third parties so that these can offer aftermarket or other data-driven services (European Commission, 2022). Another legislative initiative from the European strategy for data is the Data Governance Act (DGA)[6]. Amongst others, the DGA introduces so-called "data intermediation services". Their main purpose is data sharing through technical, legal, or other means (Article 2(2a)). According to Recital 23 such services would "enhance individual agency and in particular the individuals' control over the data relating to them" and notably help to exercise data subjects' rights under the GDPR. It is envisaged that this could be done by using personal information management tools like personal data spaces or data wallets (Slovenian Presidency of the Council of the European Union, 2021). Looking at the DGA's provisions on data intermediation services, one may conclude that Solid may be such an intermediary (CDEI, 2021).

Yet, the idea of data intermediation services is not the only trace leading in the direction of what we call the right to customization. We think that looking at current legal developments in the EU one can observe a move towards a more holistic approach that allows data subjects to exercise personalized control over their data. We believe that with our concept of a right to customization we might be able to capture the current legal, political, and technical developments, thereby making them available for a nuanced and goal-oriented discourse.

---

4 Council of the European Union, Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications) - Mandate for negotiations with the European Parliament, Brussels, 10.2.2021.

5 European Commission, Proposal for a Regulation of the European Parliament and of the Council on harmonised rules on fair access to and use of data (Data Act), Brussels, 23.2.2022, COM(2022) 68 final 2022/0047.

6 Council of the European Union, Proposal for a Regulation of the European Parliament and of the Council on European data governance (Data Governance Act) - Mandate for negotiations with the European Parliament, Brussels, 24.9.2021.

References

European Commission (2020): ‘Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, A European strategy for data’, Brussels, 19.2.2020, COM(2020) 66 final.

European Commission (2022, February 23): ‘Data Act: Commission proposes measures for a fair and innovative data economy’, press release, Brussels, retrieved April 7, 2022 from https://ec.europa.eu/commission/presscorner/api/files/document/print/en/ip_22_1113/IP_22_1113_EN.pdf.

Centre for Data Ethics and Innovation (CDEI) (2021, July 22): ‘Unlocking the value of data: Exploring the role of data intermediaries’, retrieved April 7, 2022 from https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1004925/Data_intermediaries_-_accessible_version.pdf.

Cheng, P. et al. (2019): ‘Smart Speaker privacy control - acoustic tagging for Personal Voice Assistants’, *IEEE Workshop on the Internet of Safe Things*, 23 May 2019, San Francisco, California, United States.

Choi, H., Park, J. and Jung, Y. (2018): ‘The role of privacy fatigue in online privacy behavior’, *Comput. Hum. Behav.* 81, pp. 42–51.

Custers, B. et al. (2018): ‘Consent and privacy’, in: A. Müller and P. Schaber (eds.): *The Routledge Handbook of the Ethics of Consent*, Routledge, London, 2018, pp. 247–258.

Olade, I. et al. (2020): ‘The Smart2 Speaker Blocker: An Open-Source Privacy Filter for Connected Home Speakers’, *arXiv*, arXiv:1901.04879v3.

Slovenian Presidency of the Council of the European Union (2021, October 1): ‘EU looks to make data sharing easier: Council agrees position on Data Governance Act’, press release, retrieved April 7, 2022 from https://slovenian-presidency.consilium.europa.eu/en/news/eu-looks-to-make-data-sharing-easier-council-agrees-position-on-data-governance-act/

Tamò-Larrieux, A. et al. (2021): ‘The Right to Customization: Conceptualizing the Right to Repair for Informational Privacy’, in: N. Gruschka et al. (eds.): *Privacy Technologies and Policy*, APF 2021, Lecture Notes in Computer Science, vol 12703, Springer, Cham, 2021, pp. 3–22.

van Holst, W. (2021, October 20): ‘Top system and the right to repair’, retrieved April 7, 2022 from https://edri.org/our-work/top-system-and-the-right-to-repair/.

Waldman, A.E. (2020): ‘Cognitive biases, dark patterns, and the ‘privacy paradox.’’, *Curr. Opin. Psychol. 31*, pp. 105–109.