The Right to Customization: Conceptualizing the Right to Repair for Informational Privacy

Aurelia Tamò-Larrieux[1[0000-0003-3404-7643]], Zaira Zihlmann[2[0000-0002-3592-1606]], Kimberly Garcia[1[0000-0002-4971-2944]] and Simon Mayer[1[0000-0001-6367-3454]]

[1] University of St.Gallen, Switzerland
[2] University of Lucerne, Switzerland

Abstract. Terms of use of a digital service are often framed in a binary way: Either one agrees to the service provider's data processing practices, and is granted access to the service, or one does not, and is denied the service. Many scholars have lamented these 'take-it-or-leave-it' situations, as this goes against the ideals of data protection law. To address this inadequacy, computer scientists and legal scholars have tried to come up with approaches to enable more privacy-friendly products and services. In this article, we call for a right to customize the processing of user data. Our arguments build upon technology-driven approaches as well as on the ideals of privacy by design and the now codified data protection by design and default norm within the General Data Protection Regulation. In addition, we draw upon the right to repair that is propagated to empower consumers and enable a more circular economy. We propose two technologically-oriented approaches, termed 'variants' and 'alternatives' that could enable the technical implementation of a right to customization. We posit that these approaches cannot be demanded without limitation, and that restrictions will depend on how reasonable a customization demand is.

Keywords: Right to Customization, Right to Repair, Consent; GDPR; Informational Privacy.

1 Introduction

When WhatsApp announced a change to its privacy policy in January 2021, the world reacted by downloading Signal instead [39]. This shift could be seen as the market working, yet hardly any privacy scholar would argue that the market for privacy-friendly technologies works. In fact, we have seen the many limitations of consent in the digital economy. While still a central cornerstone of data privacy regulations, multiple studies have poked holes in the concept, showing that individuals are unlikely to make rational and informed decisions about their disclosure of personal information [6][79][45][70]. One major challenge is the binary option of agreeing or not agreeing to certain data processing practices that consent provides. This is inadequate to foster the ideals of data protection law and data protection authorities (DPA) seem to be aware of the failures of 'take-it-or-leave-it'

approaches: For instance, the Norwegian DPA has issued a hefty fine to Grindr for not providing a real choice to its users [22].

In this article we call for a right to customize the data processing in a more privacy-friendly manner when reasonable to do so. We start by elaborating on the limitations of consent and how the codified principle of Privacy by Design (PbD), which is referred to as Data Protection by Design and Default (DPbDD) within the General Data Protection Regulation (GDPR), could be used as a stepping stone to enable the customization or negotiation of more fine-grained data processing operations. DPbDD demands that data controllers adhere to the data protection principles throughout the whole life cycle of data (i.e., the collection of personal data, its analysis, the use of the data for specific decisions, and its erasure). These principles include the principles concerning individual rights such as the principle of individual participation and control. Third, "Article 25 prevent[s], on its face, controllers from using technologies that collect more personal data than are strictly necessary for technological functionality or that 'leak' personal data to outsiders" [14 p. 578].

We continue by elaborating on past technologically-grounded attempts by individuals, activist groups, standardization bodies, and even industry consortia to give users more fine-grained control about aspects of their digital online privacy. This analysis shows that engineering-based regulation has failed so far, but that there is a new hope for regulation-based engineering approaches. Upon this basis, we elaborate on the right to repair, as a source of inspiration for the proposed right to customization. The right to repair has so far always related to equipment or hardware. More recently, software has been included in the bigger picture: A newly issued European Commission Report 'Circular Economy Action Plan' (2020) [30] states that the Information and Communications Technology (ICT) sector should implement a sector-wide right to repair "including a right to update obsolete software" (p. 10). This inclusion would considerably change the landscape of a right to repair and provides inspiration for the right to customization.

We elaborate on two approaches that would technically enable the right to customization: The first one focuses on deciding the type of processing at the data controllers ('variants'), while the second one focuses on deciding what data reaches which data controller ('alternatives'). However, these technical customizations must be 'reasonable'. The term reasonable is consciously broad, since different contexts will require different thresholds. While our analysis on the subject matter is not exhaustive, we elaborate on three aspects to determine the scope of reasonable customization. We end with a discussion that includes the limitations of our approach and points to further research needs.

2 Limitations of Consent in the Digital Environment

Consent is a crucial instrument for achieving informational self-determination [29][70]. Consent has been a key legal ground since the very beginning of data protection and privacy law [47]. The importance of consent in the EU data protection regime has been anchored by Article 8 of the Charter of Fundamental Rights, where

consent is identified as a basis for lawful processing of personal data [15]. Individual consent as lawful ground was also enshrined through Articles 6 and 7 of the Data Protection Directive 45/96 [23]. Its successor, the GDPR, has tightened up the requirements for establishing valid consent [49][18]. This may seem rather paradoxical in light of the fact that consent is a contested concept in European data protection legislation [79]. Given the transformative nature of consent [28] along with its connection to the idea that the data subject should have control over the use of his or her data [4], it can be very well argued that consent should (continue to) be treated as a pivotal part of the data protection regime [9]. However, many authors have pointed to its flaws, challenging the legitimacy of consent in the digital economy altogether [6][45][70].

There are multiple reasons for the limitations of consent in the digital economy. A central issue is the fact that individuals tend to accept privacy policies without reading them [18][19], thus seriously challenging the notion of 'rational and informed' decision-making. Multiple reasons contribute to this challenge: The terminologies in which privacy policies are written are difficult to understand, the time needed to do so would be exorbitant, and on top of that, there are too many of them [20][67][52]. As a consequence, users of digital services tend to provide personal data even though they indicate that they are aware of the privacy issues and concerned about data processing practices. This phenomenon is also called the 'privacy paradox' [56]. The possible reasons for this phenomenon are manifold [55], and many authors are trying to explain it by means of concepts such as privacy fatigue [17] or privacy cynicism [50]. However, there are also authors who doubt that there is evidence for such a paradox to exist [44] or challenge the concept insofar as they argue that the paradox is not so paradoxical after all [80][71]. In fact, considering that setting privacy preferences is context-dependent and users tend to be uncertain about their privacy preferences, thus they are susceptible to biases [2], which in consequence also limits the capacity to translate the received information into evidence-based privacy choices [81]. Interrelated with the user's uncertainty and the context dependence of privacy preference is the malleability, i.e., the notion that several and sometimes subtle factors can be deployed to trigger or suppress privacy concerns, which in turn influences behavior [2]. This may extend to manipulative uses of designs to frame processing practices in a certain light and manipulate users to share more personal information [80][35][38]. For instance, choices that are less privacy friendly may be presented only in a positive light (be it through wording, settings, or situations), whereas possible negative consequences for the user are intentionally omitted [57]. This is referred to as 'dark patterns' and is highly topical within various research fields [58][35][51] as well as for policymakers. Policymakers in California are even taking measures to outlaw such practices [69].

Moreover, consent is often constructed as a binary option, as in a 'take-it-or-leave-it' decision by a user [77][8]. This is especially problematic in areas where data subjects are dependent on the service of a small number of dominant online platforms, thus creating a significant power imbalance between data controllers and data subjects [18]. Individual control over personal data seems illusory in such environments, because there is no room for negotiation of the terms of use of personal data [67]. This problem is potentially exacerbated by the lack of other (privacy-friendlier) providers for the desired service [45] as well as the potential

significant social costs of not using platforms that have become the default mode of interaction [59].

In light of the above findings, the question on how this problem can be addressed arises. The legislator has not only tightened the requirements for valid consent under the GDPR, but also introduced additional provisions to strengthen the data protection rights of individuals. Among these is the principle of PbD, which could help redress the failure of consent. This can, for instance, be done by encouraging the development of systems where the consent request is designed to allow separate consent for different purposes and types of processing [19], as well as providing multi-layered and granular information to provide both accurate and understandable information to the data subject [68][66]. However, as we will show below, PbD might be an improvement, yet it is merely a stepping stone towards what we call the right to customization.

3 Privacy by Design as a Stepping Stone for a Right to Customization?

3.1 Codifying Privacy by Design

Article 25 of the GDPR codifies the principle of PbD into law. With it, overarching design principles for better privacy and security of products and services which had been around since 2009 [16] developed some legal teeth. Of course, the notion that privacy-enhancing technologies (PETs) could enable restoring the balance between data processing entities and data subjects had been around for many decades. But, as described below (see Section 4), these technologies have not become widely popular [12][13]. Nonetheless, a rich literature emerged within the field of privacy engineering [37][21][48], upon which newer proposals within the field of encoding data protection law have emerged [26].

While DPbDD under the GDPR is "less 'free'" than the original PbD principles, its inherent connection with the fundamental principles of European data protection law make it simultaneously more "ambitious and wide ranging" than PbD [12 p. 761]. In fact, Article 25 of the GDPR has been called a hollow norm [73] since the article refers back to the implementing all fundamental principles of data protection law through technical and organizational measures. The DPbDD norm distinguishes itself from other articles within the GDPR and its predecessor (the Directive 95/46/EC) by mandating the implementation of technical and organizational measures throughout the whole life cycle of data and focusing not only on security issues but the overall adherence to the principles of processing [73][14]. Moreover, Article 25 focuses "more strongly on the data subjects and their rights to technical protection measures, rather than leaving the implementation to the discretion of the data controller. The latter are called upon to ensure that certain privacy protection features are used by default" [73 p. 86].

3.2 Operalizing Data Protection by Design and Default

The norm addressees of Article 25 GDPR are clearly data controllers; they are the ones responsible for implementing measures by design and by default [14]. While this interpretation does not take into account that the design of technical infrastructures are often designed by a third party, it imposes the duty to comply with the norm to the data controller as soon as the controller actually determines the means and purposes of processing [14]. Even though the lack of broadening the norm addressee has been criticized, as it undermines "the goal of ensuring the privacy interest are fully integrated into information system architectures" [14 p. 578], the contextual dimensions of data flows and thus resulting informational privacy issues would likely make it very difficult to demand from software companies that all their products adhere to the fundamental principles of data protection by design and default. Such an interpretation would require breaking from the current approach and envisaging a more privacy engineering approach to DPbDD, which would mandate broader implementation of available privacy-enhancing technologies by developers [62]. Until now, it remains the data controllers' responsibility to mandate developers within their entity and contracted third parties to ensure that principles concerning the legality of the data processing (e.g., transparency, lawfulness, purpose limitation, information requirements), principles concerning the design of the data processing (e.g., data minimization and proportionality, disclosure and storage limitation, security, data quality), principles concerning individual rights (e.g., participation principle, accessibility, enabling erasure and object to the processing), as well as principles concerning the compliance and enforcement (e.g., accountability, documentation) are implemented by appropriate technical and organizational measures [73].

Yet, operalizing DPbDD has proven to be difficult [12][65][62][33][74]. This is due to multiple reasons, an important one being that overall European data protection law represents a compromise between different regimes which combines overarching principles with to-be-fulfilled (or justificatory) legal grounds; this duality requires data controllers to not only prove compliance with pre-determined grounds, but enables them - within boundaries - to determine how (strictly) to implement the rather vaguely defined principles that are designed to leave room for interpretation [33][74]. In fact, the principles must be interpreted taking contextual factors into account, requiring data controllers among others (1) to conduct data protection impact assessments to determine risks of processing [14], (2) to make assumptions not only about the efficacy of their risk-management strategies but also about how to determine which legal ground is appropriate in a given context (e.g., setting ad hoc hierarchies), (3) to solve conflicts within the law or generalize legal terms (which they are not equipped to do), and (4) to determine how the balancing of different interests can be encoded [33][74]. At best, encoding data protection law is thus an imperfect remedy [33][74], and it is no surprise that academics have argued that the character of privacy norms renders its implementation into code impossible [65][46].

Even if it is fair to criticize DPbDD and hardwiring data protection approaches, Article 25 has been called upon by data protection authorities—showing PbD fletching its (legal) teeth. To name just one example, in Germany a company unable to delete employee data was fined, because of non-adherence with Article 25 [5]. It remains to be seen how far Article 25 in conjunction with the fundamental principles

will be called upon by data protection authorities. Potentially, the scope of Article 25 could be enlarged to lead to what below will be described as a 'right to customization'. However, as to date such an interpretation has not been seen in practice, the following builds upon DPbDD to call for a right to customization. Instead of having to rely on an interpretation of a contested article, such a right would take the ambiguity away and lead to more legal certainty for data subjects.

3.3 Building Upon Data Protection by Design

With respect to the below outlined right to customization it is key to highlight three aspects within the duty of data controllers to implement data protection by design and default: First, with respect to the timing it is key to adhere to the data protection principles throughout the entire life cycle of data (i.e., the collection of personal data, its analysis, the use of the data for specific decisions, and its erasure). In connection with this, there is also the obligation of controllers to take into account the state of the art. In the context of technology, 'state of the art' can be defined as "the procedures, equipment or operating methods available in the trade in goods and services for which the application thereof is most effective in achieving the respective legal protection objectives" [75 p. 11]. Yet, Article 25 is silent on the meaning of 'state of the art' in its context. This may lead to the conclusion that it is a rather vague concept [62]. However, it can also be viewed as a benchmark [42] that requires data controllers to have knowledge of, and stay up to date on technological advances, meaning that as soon as technical measures and safeguards for the effective implementation of the principles and rights of data subjects are available on the market, data controllers have to either use them or implement their own equivalent or better solutions, provided that this is feasible at a reasonable expense [31][75]. Second, the principles concerning individual rights include the principle of individual participation and control. While, unlike the OECD Privacy Guidelines (1980, 2013), the GDPR does not contain one single provision ensuring participation, it is nonetheless a key ideal rooted in data protection law codified in different articles including the right to access and objection. Third, Article 25 wants to prohibit data controllers from employing technologies that collect a greater amount of data than necessary for the functionalities they offer [14]. According to Bygrave [14] Article 25 "might shape the market and technology foundations for information systems development in a privacy-friendly direction" (p. 578). However, this optimism must be contrasted with the often broad purposes that data controllers use in their privacy policies, thereby circumventing the ideal of the purpose limitation principle altogether.

Nonetheless, these requirements can be interpreted to create a stepping stone for a right to customization: The focus on the entire life cycle of data and not only the design phase and the related obligation to take into account the current technological advancements in order to ensure the effective protection of data subjects rights; the focus on individual rights and participation of data subjects; and the prohibition to collect more data than necessary sets the basis to better implement the ideals of data protection law through a right to customization.

Unlike other legal fields (e.g., copyright law and the discussion on Digital Rights Management Systems), privacy by design initiatives and the development of PETs endows a "high degree of normative and sociological legitimacy, in large part because

of its close association with furtherance of citizens' autonomy, privacy, and related civil liberties" [12 p. 766]. This is an important leverage that researchers in this field have, yet should not take for granted. As Burkert [10 p. 135] postulates: "PET design itself must be open to participatory elements. This implies that designing PETs and implementing them in social systems must involve those whom these enhancements are supposed to serve."

4 Technology Solutions to Enhance Online Privacy

4.1 The Challenges of 'Engineering-Based Regulation'

We have in the past already seen technologically-grounded attempts by individuals, activist groups, standardization bodies, and even industry consortia to implement PETs that allow users more fine-grained control about aspects of their digital online privacy. A specifically well-researched area in this domain is the automatic management of what information a user agent (e.g., a Web browser) shares with a website. For example, the Platform for Privacy Preferences Project (P3P) created a standard format that allows websites to express their privacy practices in a way that can be interpreted by user agents to provide a notice and choice approach to users. The P3P 1.0 specification[1], which defines the syntax and semantics of such privacy policies, was officially turned into a recommendation by the World Wide Web Consortium (W3C) in April 2002, updated to version 1.1[2] following community feedback on limitations and shortcomings in November 2006, and was obsoleted and retired in August 2018 as the underlying working group discontinued working on the specification. P3P enables websites to specify in concrete terms the user data they collect and process. These specifications are then automatically mapped by user agents to concrete user preferences. For instance, if a website asks for the user's telephone number, the user agent might immediately accept this request with or without notifying the user, ask the user for consent to share this specific data item, or cancel the transaction altogether. P3P furthermore allows for information requests to be tied to specific purposes, permitting more fine-grained control by the user - e.g., allowing a website to collect a specific data item, but not to share it with third parties.

P3P is implemented by having origin servers hold a policy reference file in a well-known location, by returning HTML link tags in their HTML representation, or by including a P3P HTTP header with a referrer to a P3P policy reference of the requested resource, in their HTTP response. Individual P3P policies are then required to disclose data that is collected by forms as well as the activity by background scripts that track the behavior of the user (e.g., dwelling time or clickstreams), and disclose whenever (previously consented) data is transmitted to a third party. Furthermore, policies include the purpose of the collection and processing of data, e.g., 'Tailoring' of a website or 'Contact,' where it can be specified for each of these purposes whether the processing is required ('always' required / 'opt-in' / 'opt-out'), what retention policy applies to the data item, and also to differentiate between identifiable and non-identifiable data (i.e., data that is anonymized upon collection).

---

[1] https://www.w3.org/TR/P3P/

[2] https://www.w3.org/TR/P3P11/

P3P is representative of a top-down view of creating vocabularies and specifications that are able to cover a significant part of the possible use cases but (necessarily) become very complex to implement and manage. Later, bottom-up approaches aimed to make it more amenable to websites to adhere to the user preferences they communicate. One popular mechanisms of this kind, the W3C Tracking Preference Expression[3] (known as Do Not Track; DNT), today takes the form of a HTTP header that would 'politely ask' websites to not track a user[4]. Implementing DNT headers is simple and since they are merely a binary flag (0/1), it is trivial for users to activate them through a browser setting (e.g., DNT headers are activated in private browsing modes across browsers). However, the central problem with DNT is, again, enforcement: Neither is it defined what precisely a server should do differently when receiving the header, nor are there any sanctions in place if a server does not change its behavior in response to a DNT flag. Given the body's previous experience with P3P, it is thus no surprise that the DNT header was never standardized by the W3C but merely reached the candidate recommendation stage.

Both the DNT initiative as well as P3P represent forms of 'engineering-based regulation.' This is very visible in P3P and it is seen as the main reason for its downfall: P3P policies were regarded as being too bulky and complex. The P3P working group reacted by creating more compact policies as a performance optimization in P3P 1.1. This however did not do enough to remedy the (semantic) complexity involved when creating P3P policies (for data-collection organizations), implementing P3P user agents (for Web browser implementers), and configuring preferences (for users). In addition, P3P user agents would by default exclude websites that do not publish P3P policies, thereby punishing organizations that practice high privacy standards but do not publish these as P3P, and at the same time putting large corporations with the resources to implement P3P policies at an advantage versus smaller enterprises. The most important reason for the lack of adoption of P3P, DNT, and similar systems is, however, a lack of enforcement: There are no consequences if a website does not abide by its specified policy, which undermines the core goal of this approach and also implies that companies that indeed do publish policies and abide by them are left standing without tangible benefits other than (potentially) increased user trust.

4.2 New Hope for 'Regulation-Based Engineering'

More recently, the Global Privacy Control (GPC) header[5] was introduced as a form of 'regulation-based engineering' (instead of the other way around). Far from attempting to give users the ability to customize their online privacy, GPC is specific to enabling users to opt out of the sale of their data to third parties. However, the major difference between GPC on the one side and P3P and DNT on the other is that GPC has regulatory grounding in the California Customer Privacy Act (CCPA) and in GDPR. This means that the header itself is merely a simple way of enabling users to communicate that they want to exercise their (legally guaranteed) right to opt-out of

---

[3] https://www.w3.org/TR/tracking-dnt/
[4] https://news.ycombinator.com/item?id=16110570
[5] https://globalprivacycontrol.org/

the sale of their data. So, while DNT headers merely 'politely ask,' GPC directly refers to prevailing legislation and, similar to how some online services[6] enable users to access their data based on GDPR, enables users to efficiently act upon their pre-existing rights on this basis; although GPC will need to prove itself, we see such regulation-based engineering, i.e., that technical tools facilitate the exercise of already guaranteed rights by consumers, as the only possible way forward. It is, on the basis of simple and focused solutions such as GPC, furthermore entirely conceivable that these will be extended towards the breadth and scope of P3P, while remaining fully grounded in regulation.

5 Right to Customization

5.1 Inspired by the Right to Repair: Calling for a Right to Customization

Our call for a right to customization is inspired by the right to repair. As shown above, today's data protection is confronted with a multitude of malfunctions and implementation difficulties — be it on the legal or on the technical side. However, this situation is not unique to data protection law. Consumers who aim to repair their devices face the problem that many manufacturers have made this increasingly difficult [63]. For example, Apple restricts consumers' ability to repair their devices through requiring the use of specific tools or authorized parts [61]. Against this backdrop, individuals, activists, and academics have called for manufacturers to design their products in such a way as to facilitate their repair [40].

These calls have meanwhile been heard by policymakers and the right to repair has emerged in legislation on both sides of the Atlantic [53][72][36]. The goals of such legislation are twofold: On the one hand, consumers should be empowered to repair their purchased goods (such as cars and phones) and not have to re-purchase new ones whenever minor defects arise outside of the warranty period. On the other hand, the right to repair wants to enable a more circular economy that makes more efficient use of resources. For instance, the European Parliament has issued reports and resolutions[7] demanding more durable and repairable products. With the Green Deal[8], the right to repair will likely gain further momentum.

---

[6] E.g., the service https://bitsabout.me/ in Switzerland.

[7] E.g., European Parliament report on a longer lifetime for products ((2016/2272(INI)) <https://www.europarl.europa.eu/doceo/document/A-8-2017-0214_EN.html>; European Parliament resolution of 31 May 2018 on the implementation of the Ecodesign Directive (2009/125/EC) (2017/2087(INI)) <https://www.europarl.europa.eu/doceo/document/TA-8-2018-0241_EN.html>; European Parliament, towards a more sustainable single market for business and consumers (2020/2021(INI)) <https://www.europarl.europa.eu/doceo/document/TA-9-2020-0318_EN.pdf>

[8] European Commission, Communication from the Commission, The European Green Deal (COM/2019/640 final) < https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52019DC0640&from=EN>

The focus of the right to repair has so far always been related to hardware. At the forefront of the discussion and activist claims are now electronic devices which are often cheaper to buy than to have repaired. In order to reach both goals, the empowerment of users and the promotion of a sustainable economy, in Europe, the Directive 2019/771[9] on contracts on sales of goods promotes the right to repair of goods. The term 'goods' includes 'goods with digital elements' which are defined in the Directive as "any tangible movable items that incorporate or are inter-connected with digital content or a digital service in such a way that the absence of that digital content or digital service would prevent the goods from performing their functions" (Art. 2(5)). While the focus so far has rested on products (including electronic products including 'goods with digital elements'), software has only recently been included into the bigger picture. A newly issued European Commission Report 'Circular Economy Action Plan' (2020) [30] states that the Information and Communications Technology sector should implement a sector-wide right to repair, "including a right to update obsolete software" (p. 10). This inclusion would considerably change the landscape of a right to repair and provides inspiration for the right to customization.

While a right to repair might intuitively be understood as granting the individual to make repairs on a device, the right to repair for instance in the Directive 2019/771 states this as a responsibility of the seller to conduct the repair. This makes sense, when looking at the challenges posed by the right to repair from a perspective of the goods providers. In fact, a rich discussion on closed-access repairs (i.e., consumers cannot conduct the repair themselves) versus open-access repairs can be found in the literature [72]. From a goods provider perspective, closed-access repairs are clearly preferred, as issues such as reputational ones (e.g., relating to brand management) would thereby not be inflicted. It is thus not surprising that through contractual terms only closed-access repairs are enabled by goods providers [72]. Moreover, other legal terms, such as copyright law prohibiting unauthorized circumvention of DRM also sets legal barriers to open-access repairs [53]. These legal challenges as well as sometimes offsetting prices of repair prohibit consumers from choosing freely by whom, what, and for how much to repair their products [72].

Based on the ongoing discussion and progress on a right to repair for hardware and software products and coupling this debate with the fallacies of 'take-it-or-leave-it' consent, we propose a right to customization. This right should enable users to demand the modification of a software-based service offering to better align the service with their privacy requirements. In the following, we introduce two options to technically enable such a right to customization, and subsequently discuss what types of customizations customers might reasonably expect under this right.

5.2 Technological Approaches Enabling the Customization of Consent Variants

[9] Directive (EU) 2019/771 of the European Parliament and of the Council of 20 May 2019 on certain aspects concerning contracts for the sale of goods, amending Regulation (EU) 2017/2394 and Directive 2009/22/EC, and repealing Directive 1999/44/EC (Text with EEA relevance) OJ L 136, 22.5.2019, p. 28–50.

Consider the ‘take-it-or-leave-it’ approach that WhatsApp took when introducing its privacy policy changes in early 2021. Arguably, this communication approach made even unconcerned users look into instant messaging alternatives that could bring them a better sense of safety for their personal data. Although new statements[10] about the data that WhatsApp collects and processes have been issued after the initial in-app notifications, users are still wary and have migrated to other apps, enduring the social burden of agreeing with social circles on the new instant messaging app to use, the inconvenience of starting a new conversation history (e.g., losing or backing up pictures, documents, and relevant links), learning to interact with a new user interface, and hoping that the company that owns the newly-agreed application takes a more stable approach to data privacy. However, in an ideal scenario, a user would be able to keep using the current version of WhatsApp without having to agree to the new policy, even though this could mean not having functionalities that the latest version of the app offers. Another option for a user could be to seamlessly transition to another messaging client that would have the same functionalities, user interface look and feel, and would have the ability to port conversations from WhatsApp (this references the right to data portability within GDPR).

We argue that with a right to customization in place, a user should be able to choose from a catalog of variants of an application that would be provided and curated by the data controller, the one that he, she, or they feels the most comfortable with regarding the data processing operations that this variant performs. Note that, since this gives a choice to consumers, it will not increase the total amount of data transferred and therefore will not undermine the principle of data minimization. To this end, data controllers would have the responsibility to be transparent and communicate in a clear manner about the data operations in each variant. Thus, users who enjoy highly personalized content, recommendations, and advertisement can opt for a traditional approach in which their data is transparently used to train machine learning algorithms and is probably shared with third parties that could offer additional recommendations according to their demographics. In contrast, more cautious users will be able to select a variant of the software that not only does not share their data with third-parties, but also uses techniques such as homomorphic encryption [76][3] for training machine learning algorithms, at the cost of performance or quality of the recommendations.

However, maintaining different versions of a software in order to allow users to decide the data processing activities they feel comfortable with represents a large burden on designers, software engineers, and businesses as a whole, as they would need to implement (and maintain) software that is able to provide similar services while considering such data processing customization. A way to accomplish this customization is to design and implement software on the basis of interchangeable components where, for instance, a (micro)service that analyses personal data for shopping recommendation purposes can be exchanged for one that computes such a recommendation using differential privacy [1] where noise is added to the data at the time of collection, or with a simpler service that uses heuristics without personal data.

---

10 https://faq.whatsapp.com/general/security-and-privacy/answering-your-questions-about-whatsapps-privacy-policy (last access 29.01.2021)

We expect this to encourage companies to make their software more transparent, in order to allow users to mix and match services according to their data processing preferences. Moreover, a microservice approach could enable the creation of a new marketplace, in which microservices are classified and rated according to their data processing operations. Thus, users wanting to enhance their data privacy but who do not feel educated enough to make such decisions, could follow trusted NGOs, activists, and journalists who publicly share their data processing profiles, and mimic them.

Alternatives

Another option of realizing a right to customization is to supply consumers with alternatives up front. Consider a toy robot that interacts with children and parents at home and is equipped with various sensors and processing techniques (e.g., voice and facial recognition). Different designs of the robot's processing capabilities can be envisaged, ranging from more privacy-invasive options (e.g., external processing and sharing of data with third party providers) to more privacy-friendly ones (e.g., local analysis of data). A robot made following PbD principles [33] [74], would provide a pre-installed face recognition module that runs locally in the robot. In this way, the robot would still be able to personalize its content (albeit with lower accuracy). However, requiring data controllers to create an undefined amount of variants for each software application would require mandating what such variants should look like, the data they are allowed to collect, process and store, which might put innovation at risk. Moreover, the burden in understanding and choosing the best variant would be put on the user. Conversely, favoriting a total offline approach in which the robot would host multiple variants of learning modules able to provide recommendations for every type of content (e.g., music, video, pictures, stories, etc.) would be infeasible given the limited computational capabilities of such a device. Thus, a way to maintain the same robot functionalities, while sharing data in a controlled manner, is to make users the gatekeepers to their own data. To this end, the Social Linked Data (Solid) project has been proposed. Solid [64] is a Web-based ecosystem that aims at separating data from applications. Currently, when signing up for an application such as the described robot, or for a social media service, users provide their data to a set of data controllers who store, manage, and process it in different ways. Solid provides users with a repository that contains their personal data, referred to as a podPods can be hosted online by trusted providers or by users on their own premises. Solid differs from other pod-based solutions [25] in the way that it takes advantage of technologies and protocols that already exist (e.g., Linked Data [7]) and are well-known in the computer science community. Moreover, it does not require software providers to install and run software on the user's pod, avoiding infrastructure complications. In Solid, a user grants read, write, or control permissions to an application to use explicitly identified data items in their pod. Thereby, an application obtains controlled access to the specific data that the user has explicitly decided to share with the application [11][64].

In the robot scenario, using a Solid ecosystem, a child would be identified via a WebID, which is a Uniform Resource Identifier (URI) that points to the child's personal profile containing his, her, or their data. Likes, dislikes, age, and current interests are expressed in a structured machine-readable format and are hosted in the

pod along with a set of pictures of the child's face. Moreover, users can fragment their data by topic to minimize and explicitly target the data they share with different applications. Thus, a parent can decide to share with the robot vendor the interests of the kid, but not the list of WebIDs of the kid's school friends or medical records. However, parents can decide to share medical information with a new telemedicine app that the kid's pediatrician uses for follow-ups. The permissions for applications to access a user's data are granted using a mechanism that is based on Web Access Control (WAC)[11].

Towards exercising a right to customization, solutions such as Solid could be extended with means to grant applications permissions to perform specific data processing operations (this could, for instance, be based on the catalog created by P3P). A similar mechanism as WAC could be put in place, in which users are able to create a data processing profile that specifies the type of processing they allow over their data. To this end, vocabularies such as the Data Privacy Vocabulary (DPV)[12] could be used, given that it provides a machine-readable representation of terms relevant to personal data handling, in adherence to the EU GDPR. This vocabulary specifies different processing activities with various concepts (e.g., Remove, Use) that contain various subclasses (e.g., Destruct or Erase, or Analyze, Consult, Profiling). Although this hierarchy comprises several processing activities, this is not an exhaustive list. Designers and software engineers could be in need of a not-yet-specified processing activity. Thus, it is important to stick to standardized and well-known vocabularies that are kept up to date by a community e.g., the W3C DPV community. Moreover, in order to support users in making decisions on what and how to share data with the different data controllers, a folksonomy that exposes profiles of trusted NGOs and public figures could be implemented for users to follow and mimic such profiles.

5.3 Restricting a Right to Customization to 'Reasonable Customizations'

From the discussion above it becomes clear that a right to customization could be interpreted in a way that places a (sometimes unjustifiably) large burden on businesses. The right to customization is thus not to be understood as an overarching right but must come with restrictions. We postulate that these restrictions will depend on how 'reasonable' a customization demand is. The term reasonable is consciously broad, since different contexts will require different thresholds. Clearly, the described technologies — requiring modifications at the data controller or modifying how liberally a data controller can access user data — already trigger different discussions on reasonableness. Demanding the creation of variants is costly, time-intensive, and against the business interests of data controllers and must thus be weighed against the interests of data subjects to customize the processing of their personal data. While the analysis that follows is by no means exhaustive, it provides insights on how to determine what falls under 'reasonable customizations'. Needless to say, it would be desirable to have a set of objective criteria, so as to prevent interpretations of the

[11] https://www.w3.org/wiki/WebAccessControl
[12] https://dpvcg.github.io/dpv/

criterion ‘reasonable’ that would result in a worsening of the position of the end user. However, for the establishment of concrete criteria, further discussion is essential. Such a discussion cannot be held without involving more stakeholders to the debate, including researchers from other fields, activists, industry representatives, and policymakers.

First, we can learn from the discussion on the right to repair. The Directive 2019/771, for instance, states in Recital 48: “The consumer's choice between repair and replacement should only be limited where the option chosen would be legally or factually impossible or would impose costs on the seller that would be disproportionate, compared to the other option available.” This shows clearly that there are costs that are disproportionate, especially when the costs of repair would be unreasonably high compared to other alternatives [54] (ECJ, C-65/09 and C-87/09). Moreover, repair cost can be attributed to the customer. Also the right for customization could, especially in the case of variant-building by data controllers, come with a cost that is passed on to users. While this would enable more privacy-aware users to pay for customizing consent, others might not do so. Of course, such a development could lead to even greater disparity between the ‘privacy-haves’ and ‘privacy-have-nots.’

Second, we can learn from debates surrounding the right to data portability enshrined in Article 20 GDPR, which aims to enhance user control and minimize lock-in effects by facilitating the transfer of data. Despite that many aspects of Article 20 GDPR leave room for interpretation [41], it, as well as the discussions about its shortcomings, can serve as inspiration for possible constraints on the right to customization. This is due to the circumstance that enabling data portability imposes additional costs and efforts on data controllers (with some arguing that it would especially negatively affect small and medium-sized enterprises and would serve as a barrier to market entry, resulting in a negative impact on innovation and competition [78]). Accordingly, limits to this right must reasonably exist. Recital 68 of the GDPR states that the data subject should only have the right to have personal data transferred directly from one controller to another if this is technically feasible. From this it follows that since there is no obligation to establish or maintain processing systems that are technically compatible with those of other controllers, the full exercise of users' right to data portability may be restricted by data controllers if they demonstrate that their organization's technological deployment level makes direct transfer of data to another controller technically infeasible [24]. However, demonstrating such infeasibility might prove hard. Moreover, one has to consider that “what is technically feasible for one data controller might not be technically feasible for another data controller” [27 p. 13]. Against this background, it can be argued that restrictions should be asymmetric, i.e., the obligations applicable to a company would be based on its market share or the scope of its activities. Consequently, entities that have significant market power from a competition law perspective would be subject to stricter obligations to provide for data portability [34]. Lastly, the right to data portability needs to be balanced against other rights. According to Article 20(4) of the GDPR, the right to data portability shall not adversely affect the rights and freedoms of others. This also includes the freedom to conduct a business of data controllers [24].

Finally, the freedom to conduct business should set limits to the right to customization as latter would make the development and deployment of technology more costly and thus harder for providers to compete in the market. The freedom to conduct business (as enshrined in Article 16 of the Charter of Fundamental Rights), includes the right of any company or individual to be able to freely use its economic, technical, and financial resources ([60] with reference to ECJ, C-314/12). Yet, also the freedom to conduct a business is not an absolute right but can be subject to restrictions, "provided that such restrictions correspond to objectives of general interest pursued by the EU and do not constitute a disproportionate and intolerable interference in relation to the aim pursued, impairing the very substance of the rights guaranteed" [32 p. 23]. How to determine what are reasonable customizations and what boundaries the freedom to conduct business sets will have to be evaluated on a case-by-case basis. Potentially, courts could draw insights from other domains, such as in copyright enforcement, where platforms can be required to implement at their own expense upload filters, but where courts have also set limits to such requirements (e.g., SABAM v. Netlog).

6 Discussion and Conclusion

In this article, we have started by describing the limitations of consent in the digital economy and how DPbDD could be seen as a stepping stone for demanding the customization of data processing practices. However, because such an interpretation of DPbDD so far does not exist, we introduce the concept of the (reasonable) right to customization. This right, understood as an individual right to be included within an amended data protection regulation, would empower data subjects to demand more customizable services from data controllers. While acknowledging that technology-driven solutions so far have failed to provide greater user control, there is a new hope for regulation-based engineering approaches that have been developed world-wide. Upon this basis, and inspired by the right to repair which is being interpreted more broadly to include software updates in recent policy making documents, we postulate the right to reasonable customization. Both, the right to repair and the right to customization strive to enable better user control over devices or software and strive to fulfill greater ideals, such as sustainable developments, and privacy-friendly technology developments. Moreover, the stakeholders are similar: On the one hand, individuals (striving for a green planet or more privacy-friendly environments) and on the other hand, large corporations, wanting to continue with their current business model (e.g., increasing revenue, profiling for targeted advertising and content).

A central question that remains is: How does the right to customization address the failures of consent mentioned above in practice? The main advantage of our conceptualization of the right to repair approach is that it moves away from the binary or 'take-it-or-leave-it' approach; this approach is dominant with consent, but becomes also apparent when processing is necessary for the performance of a contract or when legitimate interests of a (big tech) data controller are evoked. Specifically, the right to customization demands from data controllers to provide either reasonable variants or alternatives to users. This reasoning is in line not only with the aspiration of DPbDD

but also currently enacted individual rights such as the right to data portability. In addition, the right to customization can permit the creation of more open ecosystems, with the hope that these lead to more transparent systems that enable users to engage with it. It could also incentivize data controllers to be more transparent about their services (and variants thereof), and to create more privacy-friendly variants of their services from the start, in order not to risk having users demand their right to customization. Such right to customization requests would then require a re-design of data processing practices, which would be more costly than having thought about them before a product or service launch, thus supporting the core ideals of PbD. In that sense, the right to customization might address some of the information asymmetries and lack of control discussed above (see Section 2). Yet, the right to customization is by no means an ultimate remedy to those challenges, as they are systemic to the current digital economy. For instance, enabling more granular designs of services is not going to prevent the trend of manipulating users to choose the data controller's favorite option over others (in the extreme by means of dark patterns). In addition, critics will likely point out that the proposed technical solutions to enable a right to customization fall within the dream of 'techno-solutionism,' which stands for finding technical remedies to societal problems without taking the bigger picture into account [43]. However, as discussed in Section 4, we believe that regulation-based engineering (i.e., engineering that facilitates the exercise of rights) is in principle better able to achieve the objectives of the proposed right to customization. Moreover, looking at the current draft of the ePrivacy Regulation[13], one can observe that EU policymakers are aware of the pressing issues concerning end-user consent and are seeking to address the problem. Recital 20a states that "[i]mplementation of technical means in electronic communications software to provide specific and informed consent through transparent and user-friendly settings, can be useful to address this issue. Where available and technically feasible, an end user may therefore grant, through software settings, consent to a specific provider for the use of processing and storage capabilities of terminal equipment for one or multiple specific purposes across one or more specific services of that provider." This approach seems to be heading in the same direction as the herein proposed right to customization. However, a right to customization would go a step further by not only providing the possibility to grant or deny consent through software settings, but by allowing users to mix and match services according to their data processing preferences.

Moreover, while striving for more user control is not per se a faulty quest, we are continuing to try to solve systemic and collective problems of the digital economy through individual means. To steer away from this problem, we see a need to re-calibrate such approaches and enable more community and collective redress actions. For instance, we need to enable activists of NGOs to facilitate access to widely applicable customizations to users. Hence, similar to how 'repair cafés' enable users to exercise their right to repair by giving them access to and support by enthusiasts, online or offline 'customization communities' would help individuals to

[13] Council of the European Union, Draft regulation concerning 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) – Council mandate<https://data.consilium.europa.eu/doc/document/ST-6087-2021-INIT/en/pdf>

exercise their right to customization. This could induce a folksonomy-based approach to the customization of frequently used services, i.e., a situation where specific customization solutions would be shared among a community of participants.

References

1. Abadi, M., Chu, A., Goodfellow, I., McMahan, H.B., Mironov, I., Talwar, K., and Zhang, L.: Deep learning with differential privacy. In: Proceedings of the ACM SIGSAC Conference on Computer and Communications Security, pp. 308-318. Association for Computing Machinery (2016).
2. Acquisti, A., Brandimarte, L., and Loewenstein, G.: Privacy and human behavior in the age of information. Science 347(6221), 509-514 (2015).
3. Agrawal, N., Binns, R., Van Kleek, M., Laine, K. and Shadbolt, N.: Exploring Design and Governance Challenges in the Development of Privacy-Preserving Computation. arXiv preprint arXiv:2101.08048 (2021).
4. Article 29 Working Party: WP29 Opinion 15/2011 on the definition of consent (WP 187), Adopted 13 July 2011 <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2011/wp187_en.pdf> (2011).
5. Berliner Beauftragte für Datenschutz und Informationsfreiheit: Berliner Datenschutzbeauftragte verhängt Bussgeld gegen Immobiliengesellschaft, 5 November 2019 <https://www.datenschutz-berlin.de/fileadmin/user_upload/pdf/pressemitteilungen/2019/20191105-PM-Bussgeld_DW.pdf> (2019).
6. Bietti, E.: Consent as a Free Pass: Platform Power and the Limits of the Informational Turn. Pace Law Review 40, 307-397 (2020).
7. Bizer, C., Heath, T., and Berners-Lee, T.: Linked data: The story so far. In: Semantic Services, Interoperability and Web Applications: Emerging Concepts, pp. 205-227. IGI global (2011).
8. Borgesius, F., Kruikemeier, S., Boerman, S., and Helberger, N.: Tracking Walls, Take-It-Or-Leave-It Choices, the GDPR, and the ePrivacy Regulation. European Data Protection Law Review 3, 353–368 (2017).
9. Brownsword, R.: Consent in Data Protection Law: Privacy, Fair Processing and Confidentiality. In: Gutwirth, S., Poullet, Y., de Hert, P., de Terwangne, C., and Nouwt, S. (eds.) Reinventing Data Protection?, pp. 83-110. Springer, Dordrecht (2009).
10. Burkert, H.: Privacy-Enhancing Technologies: Typology, Critique, Vision. In: Agre, P. and Rotenberg, M. (eds.), Technology and Privacy: The New Landscape, pp. 126-143. MIT Press,. Boston, MA (1997).
11. Buyle, R., Taelman, R., Mostaert, K., Joris, G., Mannens, E., Verborgh, R., and Berners-Lee, T.: Streamlining governmental processes by putting citizens in control of their personal data. In: International Conference on Electronic Governance and Open Society: Challenges in Eurasia, pp. 346-359. Springer, Cham (2019).
12. Bygrave, L. A.: Hardwiring Privacy. In: Brownsword, R., Scotford, E., and Yeung, K. (eds.) The Oxford Handbook of Law, Regulation, and Technology, pp. 754-775. Oxford University Press, Oxford (2017).
13. Bygrave, L. A.: Privacy-enhancing Technologies: Caught Between a Rock and a Hard Place. Privacy Law & Policy Reporter 9, 135-137 (2002).

14. Bygrave, L. A.: Article 25 Data protection by design and by default. In: Kuner, C., Bygrave, L. A., and Dockyes, C. (eds.), The EU General Data Protection Regulation (GDPR): A Commentary, pp. 571-581. Oxford University Press, Oxford (2020).
15. Carolan, E.: The continuing problems with online consent under the EU's emerging data protection principles. Computer Law & Security Review 32(3), 462–473 (2016).
16. Cavoukian, A.: Privacy by Design: The 7 Foundational Principles (August 2009; revised January 2011) <https://www.ipc.on.ca/wp-content/uploads/Resources/7foundationalprinciples.pdf> (2011).
17. Choi, H., Park, J., and Jung, Y.: The Role of Privacy Fatigue in Online Privacy Behavior. Computers in Human Behavior 81, 42–51 (2018).
18. Clifford, D., Graef, I., and Valcke, P.: Pre-formulated Declarations of Data Subject Consent: Citizen-Consumer Empowerment and the Alignment of Data, Consumer and Competition Law Protections. German Law Journal 20(5), 679-721 (2019).
19. Custers, B., Dechesne, F., Pieters, W., Schermer, B., and van der Hof, S.: Consent and Privacy. In: Müller, A., and Schaber, P. (eds.), The Routledge Handbook of the Ethics of Consent, pp. 247-258. Routledge, London (2018).
20. Custers, B. Click here to consent forever: Expiry dates for informed consent. Big Data & Society 3(1), 1-6 (2016).
21. Danezis, G., Domingo-Ferrer, J., Hansen, M., Hoepman, J.-H., Le Métayer, D., Tirtea, R., and Schiffner, S.: Privacy and Data Protection by Design - From Policy to Engineering, European Union Agency for Network and Information Security, ENISA, 12 January 2015 <www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/privacy-and-data-protection-by-design> (2014).
22. Datatilsynet: Advance notification of an administrative fine, 20/02136-5, 24 January 2021 <https://www.datatilsynet.no/contentassets/da7652d0c072493c84a4c7af506cf293/advance-notification-of-an-administrative-fine.pdf> (2021).
23. De Hert P., and Papakonstantinou, V.: The new General Data Protection Regulation: Still a sound system for the protection of individuals?. Computer Law & Security Review 32(2), 179-194 (2016).
24. De Hert, P., Papakonstantinou, V., Malgieri, G., Beslay, L., and Sanchez, I.: The right to data portability in the GDPR: Towards user-centric interoperability of digital services. Computer Law & Security Review 34(2), 193-203 (2018).
25. De Montjoye, Y.A., Shmueli, E., Wang, S.S., and Pentland, A.S.: Openpds: Protecting the privacy of metadata through safeanswers. PloS one, 9(7), p.e98790 (2014).
26. De Oliveira Rodrigues, C. M., Gonçalves de Freitas, F. L., Spósito Barreiros, E. F., Ribeiro de Azevedo, R., and de Almeida Filho, A. T.: Legal ontologies over time: A systematic mapping study, Expert Systems with Applications, 130, 12-30, (2019).
27. Diker Vanberg, A.: The Right to Data Portability in the GDPR: What Lessons Can Be Learned from the EU Experience?. Journal of Internet Law 21, 11-19 (2018).
28. Edenberg, E., and Jones, M. L.: Analyzing the legal roots and moral core of digital consent. New Media & Society 21, 1804–1823 (2019).
29. Efroni, Z., Metzger, J., Mischau, L., and Schirmbeck, M.: Privacy Icons: A Risk-Based Approach to Visualisation of Data Processing. European Data Protection Law Review 5(3), 352-366 (2019).
30. European Commission: Circular Economy Action Plan: For a cleaner and more competitive Europe. <https://ec.europa.eu/environment/circular-economy/pdf/new_circular_economy_action_plan.pdf> (2020).

31. European Data Protection Board (EDPB): Guidelines 4/2019 on Article 25 Data Protection by Design and by Default, Adopted 23 November 2019 <https://edpb.europa.eu/sites/edpb/files/consultation/edpb_guidelines_201904_dataprotection_by_design_and_by_default.pdf> (2019).
32. European Union Agency for Fundamental Rights (FRA): Freedom to conduct a business: exploring the dimensions of a fundamental right <https://fra.europa.eu/sites/default/files/fra_uploads/fra-2015-freedom-conduct-business_en.pdf> (2015).
33. Garcia, K., Zihlmann, Z., Mayer, S., and Tamo-Larrieux, A.: Towards Privacy-Friendly Smart Products. Manuscript submitted for publication, (2021) <https://www.alexandria.unisg.ch/262898/>
34. Graef, I.: The opportunities and limits of data portability for stimulating competition and innovation. Competition Policy International - Antitrust Chronicle 2, 1-8 <https://pure.uvt.nl/ws/portalfiles/portal/45777953/CPI_Graef_data_portability.pdf> (2020).
35. Gray, C., Santos, C., Bielova, N., Toth, M., and Clifford, D.: Dark Patterns and the Legal Requirements of Consent Banners: An Interaction Criticism Perspective. arXiv preprint arXiv: arXiv:2009.10194 (2020).
36. Grinvald, L.C., and Tur-Sinai, O.: Intellectual Property Law and the Right to Repair. Fordham Law Review 88(1), 64-128 (2019).
37. Gürses, S., Troncoso, C., and Diaz, C.: Engineering Privacy by Design. Fourth Conference on Computers, Privacy and Data Protection, 25–27 January 2011 <www.cosic.esat.kuleuven.be/publications/article-1542.pdf> (2011).
38. Hartzog, W.: Privacy's Blueprint The Battle to Control the Design of New Technologies. Harvard University Press, Cambridge, Massachusetts (2018).
39. Hern, A.: WhatsApp loses millions of users after terms update. The Guardian, 24 January 2021 <https://www.theguardian.com/technology/2021/jan/24/whatsapp-loses-millions-of-users-after-terms-update> (2021).
40. Hernandez, R., Miranda, C., and Goñi, J.: Empowering Sustainable Consumption by Giving Back to Consumers the 'Right to Repair'. Sustainability 12(3), 850 (2020).
41. Janal, R.: Data Portability - A Tale of Two Concepts. JIPITEC 8, 59-69 (2017).
42. Jasmontaite, L., Kamara, I., Zanfir-Fortuna, G., and Leucci, S.: Data Protection by Design and by Default: Framing Guiding Principles into Legal Obligations in the GDPR. European Data Protection Law Review 4, 168-189 (2018).
43. Johnston, S. F.: The Technological Fix as Social Cure-All: Origins and Implications, IEEE Technology and Society Magazine, March (2018).
44. Kokolakis, S.: Privacy attitudes and privacy behaviour: a review of current research on the privacy paradox phenomenon. Computers & Security 64, 122–134 (2017).
45. Koops, B.-J.: The Trouble with European Data Protection Law. International Data Privacy Law 4(4), 250–261 (2014).
46. Koops, B.-J., and Leenes, R.: Privacy regulation cannot be hardcoded. A critical comment on the 'privacy by design' provision in data-protection law, International Review of Law, Computers and Technology, 159-171 (2014).
47. Kosta, E.: Consent in European Data Protection Law. Martinus Nijhoff Publishers, Leiden (2013).
48. Kostova, B., Gürses, S., and Troncoso, C.: Privacy Engineering Meets Software Engineering. On the Challenges of Engineering Privacy ByDesign, arXiv preprint arXiv:2007.08613 (2020).

49. Kotschy, W.: Article 6 Lawfulness of processing. In: Kuner, C., Bygrave, L. A., and Dockyes, C. (eds.), The EU General Data Protection Regulation (GDPR): A Commentary, pp. 321-344. Oxford University Press, Oxford (2020).
50. Lutz, C., Hoffmann, C. P., and Ranzini, G.: Data capitalism and the user: An exploration of privacy cynicism in Germany. New Media & Society 22(7), 1168–1187 (2020).
51. Mathur, A., Acar, G., Friedman, M., Lucherini, E., Mayer, J.R., Chetty, M., and Narayanan, A.: Dark Patterns at Scale. In: Proceedings of the ACM on Human-Computer Interaction, pp. 1-32. arXiv preprint arXiv:1907.07032 (2019).
52. McDonald, A. M., and Cranor, L. F.: The cost of reading privacy policies. I/S A Journal of Law and Policy for the Information Society 4, 540–565 (2008).
53. Montello, S.: The Right to Repair and the Corporate Stranglehold over the Consumer: Profits over People. Tulane Journal of Technology and Intellectual Property 22, 165-184 (2020).
54. Morais Carvalho, J.: Sale of Goods and Supply of Digital Content and Digital Services – Overview of Directives 2019/770 and 2019/771. SSRN <https://ssrn.com/abstract=3428550> (2019).
55. Mourey, J. A., and Waldman, A.E.: Past the Privacy Paradox: The Importance of Privacy Changes as a Function of Control and Complexity. Journal of the Association for Consumer Research 5(2), 162-180 (2020).
56. Norberg, P. A., Horne, D. R., and Horne, D. A.: The privacy paradox: Personal information disclosure intentions versus behaviors. Journal of Consumer Affairs 41, 100-126 (2007).
57. Norwegian Forbrukerrådet: Deceived by design: How tech companies use dark patterns to discourage us from exercising our rights to privacy <https://fil.forbrukerradet.no/wp-content/uploads/2018/06/2018-06-27-deceived-by-design-final.pdf> (2018).
58. Nouwens, M., Liccardi, I., Veale, M., Karger, D., and Kagal, L.: Dark Patterns after the GDPR: Scraping Consent Pop-ups and Demonstrating their Influence. In: Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems, pp. 1-13. arXiv preprint arXiv: 2001.02479 (2020).
59. Raynes-Goldie, K.: Aliases, creeping, and wall cleaning: understanding privacy in the age of Facebook. First Monday 15(1) <https://firstmonday.org/ojs/index.php/fm/article/view/2775> (2010).
60. Reda, J., and Selinger, J.: Article's 17's impact on freedom to conduct a business - part 2, Kluwer Copyright Blog, 21 January 2021 <http://copyrightblog.kluweriplaw.com/2021/01/19/article-17s-impact-on-freedom-to-conduct-a-business-part-2/> (2021).
61. Rosa-Aquino, P.: Fix, or Toss? The 'Right to Repair' Movement Gains Ground. New York Times, 23 October 2020 <https://www.nytimes.com/2020/10/23/climate/right-to-repair.html> (2020).
62. Rubinstein, I., and Good, N.: The trouble with Article 25 (and how to fix it): the future of data protection by design and default. International Data Privacy Law 10(1), 37–56 (2020).
63. Šajn, N.: Consumers and repairs of products, Briefing of European Parliamentary Research Service, <https://www.europarl.europa.eu/RegData/etudes/BRIE/2019/640158/EPRS_BRI(2019)640158_EN.pdf > (2019).
64. Sambra, A.V., Mansour, E., Hawke, S., Zereba, M., Greco, N., Ghanem, A., Zagidulin, D., Aboulnaga, A., and Berners-Lee, T.: Solid: a platform for decentralized social applications based on linked data. MIT CSAIL & Qatar Computing Research Institute, Tech. Rep. (2016).

65. Schartum, D.: Making Privacy by Design Operative, International Journal of Law and Informational Technology 24, 151-175 (2016).
66. Schaub, F., Balebako, R., Durity, A., and Cranor, L.: A Design Space for Effective Privacy Notices. In: Selinger, E., Polonetsky, J., and Tene, O. (eds.) The Cambridge Handbook of Consumer Privacy, pp. 365-393. Cambridge University Press, Cambridge (2018).
67. Schermer, B., Custers, B., and van der Hof, S.: The crisis of consent: how stronger legal protection may lead to weaker consent in data protection. Ethics and Information Technology 16, 171–182 (2014).
68. Schiffner, S., Berendt, B., Siil, T., Degeling, M., Riemann, R., Schaub, F., Wuyts, K., Attoresi, M., Gürses, S., Klabunde, A., Polonetsky, J., Sadeh, N., and Zanfir-Fortuna, G.: Towards a roadmap for privacy technologies and the general data protection regulation: A transatlantic initiative. In: Proceedings of the Annual Privacy Forum 2018, pp. 24-42 (2018).
69. Simonite, T.: Lawmakers Take Aim at Insidious Digital 'Dark Patterns'. WIRED, 29. January 2021 < https://www.wired.com/story/lawmakers-take-aim-insidious-digital-dark-patterns/>
70. Solove, DJ.: Privacy self-management and the consent dilemma. Harvard Law Review 126, 1880–1903 (2013).
71. Solove, DJ.: The Myth of the Privacy Paradox. George Washington Law Review 89, 1-42 (2021).
72. Svensson, S., Richter, J. L., Maitre-Ekern, E., Pihlajarinne, T., Maigret, A., and Dalhammer, C.: The Emerging 'Right to Repair' legislation in the EU and the U.S. Paper presented at Going Green CARE Innovation < https://portal.research.lu.se/portal/files/63585584/Svensson_et_al._Going_Green_CARE_INNOVATION_2018_PREPRINT.pdf> (2018).
73. Tamò-Larrieux, A.: Designing for Privacy and Its Legal Framework: Data Protection by Design and Default for the Internet of Things. Springer, Cham (2018).
74. Tamò-Larrieux, A., Mayer, S., and Zihlmann, Z.: Softcoding not Hardcoding Privacy. Workshop paper presented at the Digital Legal Talks <https://www.alexandria.unisg.ch/cgi/users/home?screen=EPrint::View&eprintid=262254#t> (2020).
75. Teletrust and ENISA: IT Security Act (Germany) and EU General Data Protection Regulation: Guideline "state of the art" technical and orgnaisational measures <https://www.teletrust.de/fileadmin/docs/fachgruppen/ag-stand-der-technik/2020-10_TeleTrusT_Guideline_State_of_the_art_in_IT_security_EN.pdf> (2020).
76. The Royal Society: Protecting Privacy in Practice: The Current Use, Development and Limits of Privacy Enhancing Technologies in Data Analysis. Technical Report. The Royal Society (2019).
77. Utz, C.; Degeling, M., Fahl, S., Schaub, F., and Holz, T.: (Un)informed Consent: Studying GDPR Consent Notices in the Field. In: Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security (CCS '19), pp. 973–990 (2019).
78. Vanberg, A., and Ünver, M.: The right to data portability in the GDPR and EU competition law: odd couple or dynamic duo?. European Journal of Law and Technology 8(1), 1-22 (2017).
79. Van Hoboken, J. V. J.: Privacy Disconnect. In: Human Rights in the Age of Platforms, pp. 255-284. The MIT Press, Cambridge (2019).
80. Veltri, G. A., and Ivchenko, A.: The impact of different forms of cognitive scarcity on online privacy disclosure. Computers in Human Behavior 73, 238–246 (2017).
81. Waldman A. E.: Cognitive biases, dark patterns, and the 'privacy paradox'. Current opinion in psychology 31, 105–109 (2020).