Saving the web by decentralizing data networks? A socio-technical reflection on the promise of decentralization and personal data stores

Peter Mechant
imec-mict-UGent
Ghent, Belgium
0000-0002-5283-5806

Ralf De Wolf
imec-mict-UGent
Ghent, Belgium
0000-0002-2586-4150

Mathias Van Compernolle
imec-mict-UGent
Ghent, Belgium
0000-0002-6194-1168

Glen Joris
imec-mict-UGent
Ghent, Belgium
0000-0002-4202-2641

Tom Evens
imec-mict-UGent
Ghent, Belgium
0000-0002-7274-7432

Lieven De Marez
imec-mict-UGent
Ghent, Belgium
0000-0001-7716-4079

***Abstract*—In this article we elaborate on Personal Information Management Systems (PIMS) or Personal Data Stores (PDS) that provide a person with affordances for managing his/her personal data, giving him/her granular control over the data captured about him/her, and over how that data is shared and used. We examine the promise of PDS-enabled data cooperatives from a socio-technical approach by critically unpacking the current discourse on data activism and related concepts such as data cooperatives, data collaboratives or data bazaars in the context of PDSs. We highlight critical reflections on user empowerment, power symmetries and user appropriation. While we see promise in a collective approach to the management of (personal) data, as it may reorient markets and change who benefits from datafication, we point out that further research into the potential obstacles or hurdles that hinder the implementation of data cooperatives in a PDS-ecology and into what consumers think about these and other possible data management models, is needed.**

***Keywords*—personal data stores, appropriation, empowerment, power assymmetries**

I. Introduction

The internet has become increasingly pervasive and critical for societies, systems, organizations, and individuals. The International Telecommunication Union (ITU) estimates that at the end of 2019, about 51% of the global population were using the Internet which is an increase of 25% in one decade [1]. At the same time the internet has become subject to critical concerns, especially with regards to personal data management. For example, both qualitative [2]–[4] as well as quantitative research [5]–[7] has shown that people perceive the collection, usage, and sharing of personal information online as a severe problem. The growing attention in literature for concepts such as digital resignation [8], data compliance [9], privacy fatigue [10], or 'assetization of personal data' [11] also expresses these concerns.

Today's societies frame personal data (management) within broader imaginaries of personal data as the key driver of twenty-first-century economies [11]. Personal data is put central to informational capitalism that thrives on the transformation of information into a commodity. In informational capitalism, however, data is siloed away from people. Data subjects do not know what data about them is being stored, nor do they have control over how it is used, or by whom. Van Dijck [12] refers to this technological trend that turns many aspects of people's life into data as datafication. Datafication in informational capitalism serves a dual role and is both a process of production and a form of injustice. In this context, [11], [13], warn against a shift towards data rentiership, i.e., "the extraction of value through different modes of ownership and control over resources and assets" [11, p. 470]. Data, as assets that are essential for the functioning of critical infrastructures such as transportation or public administration, are used to create value by means of ownership and control, thus creating power asymmetries in how data and the means of knowledge production are distributed.

Data activism denounces these current power asymmetries [14]. *Proactive* data activism, specifically, tackles unjust data practices by putting forward 'decentralized data networks' and 'data cooperatives' to afford people with meaningful agency over their personal data (and over how this data is gathered and processed). Personal Data Spaces or Personal Data Stores (PDS) embrace these design principles and aim explicitly at decentralization; they provide a person with controls for managing his/her personal data, giving him/her granular control over the data captured about him/her, and over how that data is shared and used. For example, using SOLID-based applications [15], users can conveniently switch between data storage providers and application providers. Third parties such as companies can access a person's data via a PDS, with permission, through a secure link for a specific task (e.g., processing a loan application or delivering a personalized ad).

While PDSs are a key element for effectively realizing decentralized data networks, PDSs can also be considered as social imaginaries of how the data economy should work. They enable people to easily reuse their data by providing more control and transparency on how this data is stored and shared. In the case of SOLID, PDSs are part of a network of linked-data applications that are completely decentralized and fully under users' control rather than controlled by others, thus promoting a new capacity to act towards data. PDSs are grounded in the idea that with enough information presented in the right way, users can overcome barriers in managing their personal data that are structural and systemic in nature (the logic of 'privacy self-management'). As such, PDSs posit datafication as a given; "(…) their features and development rationales exemplify attempts to intensify datafication" [16, p. 635].

Current processes of datafication and data appropriation are often opaque and neglect user's agency. In addition, the many data leakages, and poorly managed data infrastructures by (commercial) companies pave the road to sustainable

978-1-6654-1645-0/21/$31.00 ©2021 IEEE

alternatives. The goal of this article is to examine the promise of PDS-enabled data cooperatives from a socio-technical approach. In what follows, we will critically unpack the current discourse on data activism and related concepts such as data cooperatives, data collaboratives or data bazaars in the context of PDSs. We highlight critical reflections on user empowerment (e.g., 'To what extent do PDSs and decentralized data networks empower instead of making users more responsible?'), power symmetries (e.g., 'Will PDSs prevent third parties form collecting and exploiting user data?') and user appropriation (e.g., 'Are people willing and able to use PDSs?'). To be fair, we neither can nor intend to tackle all questions on PDSs and data activism. Rather, we want to extend, and hopefully shape, further the current discussions by eliciting the role of users and society. Indeed, our socio-technical approach rejects the idea or presumption that a technology (here PDSs) can fix or change a structural problem (cfr. technological solutionism).

II. Literature

A. *Decentralised storage of personal information, data cooperatives and data collaboratives*

As described above, proactive data activism, tries to tackle unjust data practices by putting forward 'decentralized data networks'. Claims about how decentralised storage of data could be an important response to problems of autonomy of data subjects and power asymmetries in data ecologies, are not new see e.g., [17] but are increasingly challenged by startup or research companies bringing to market actual applications supporting decentralised storage of personal information, often called Personal Data Spaces (PDS), e.g., Cozy Cloud, Meeco, OpenPDS or SOLID (https://solidproject.org/).

Proactive data activism can be situated in the context of Web 3.0 because - while Web 1.0 can be considered as system of human cognition and Web 2.0 as system of human communication - Web 3.0 adds the Marxian idea of collective cooperative production and Tönnies' idea of communities" to online sociability [18]. In Web 3.0, as a system of human cooperation, it is the internet itself that offers the services, and not a few big commercial parties. Web 3.0 internet-based services emphasize a machine-facilitated understanding of information and a decentralised web that challenges the dominance of the big commercial parties. They offer an alternative to hyper-concentrated data centers and cloud providers while guaranteeing better protection of user privacy and data sovereignty.

In this context PDS should enable individuals to "have an easy way to see where data […] goes, specify who can use it, and alter these decisions over time" (https://mydata.org/what-we-want) and should create an ecosystem where individuals control the sharing of their data between interoperable data sources and endpoints [14]. PDS enable individuals to easily reuse their data by providing more control and transparency on how this data is stored and shared.

In this article we will focus on PDSs enabled by SOLID. SOLID is a platform for linked-data applications that are completely decentralized and fully under users' control rather than controlled by others. Using a recently developed taxonomy for data ecosystems [19], that starts from three meta-dimensions (economic, technical and governance), SOLID can be described as a PDS system that supports a data ecosystem that functions in different domains overlapping the blurred boundaries between science, government and industry and serving innovation, interaction as well as transaction in a decentralized manner (economic); using an open and distributed infrastructure (technical) and supporting actors in the data ecosystem that are loosely coupled while control of the essential data resources is decentralized (governance).

Personal data stores (PDS) are a key technical component in SOLID; they allow an individual to control his or her own data in an individual 'data safe'. Companies can access a person's data, with permission, through a secure link for a specific task. De Bot & Haegemans [20] distinguish three important access or data sharing patterns that SOLID enables; (i) the Direct Data Exchange with Consent (DC) Pattern describes a direct exchange of data between the source and the recipient in which the data subject instructs the data source to share the data with the recipient, (ii) the Indirect Data Exchange with Provision (IP) Pattern describes an indirect exchange of data between the source and the recipient in which the data subject asks the data source to share the data with him/her and thereafter shares his/her data with the recipient, and (iii) the Direct Data Exchange with Feedback (DF) Pattern describes a direct exchange of data between the source and the recipient with no involvement at all of the data subject (he/she is however informed about this exchange).

These data sharing patterns should better protect personal data from access by third parties. They use compartmentalized data storage and computation to prevent apps from interacting with data inappropriately and can create opportunities for users to gain more insights from their data.

Proactive data activism tries to prevent unjust data practices by putting forward, amongst others, so-called 'data cooperatives'. Such an approach tries to tackle datafication and the current shift towards data rentiership on a collective instead of individual basis. PDSs are used to aggregate data and to develop a cooperative data sharing approach and function as a solution to the growing sense of powerlessness people feel in the current data ecology. Data cooperatives' main purpose is then to ensure the stewardship of data for the benefit of their individual members. Such data cooperatives differ from 'data commons' in that in a data common, the common data resource is undivided (i.e., all members have equal rights), while in a data cooperative, data resources belong to individual members and are brought into the cooperative [21]. Below, we will unpack key concepts related to this idea of 'data cooperatives' as a construct to afford people meaningful agency over their personal data.

In 'Data cooperatives for pandemic times', [22] suggest that the economic resource of data should be organized locally through data cooperatives in the form of a member-owned data management system. The authors continue by defining a cooperative as "(…) an autonomous association of persons united voluntarily to meet their common economic, social, and cultural needs and aspirations through a jointly-owned and democratically-controlled enterprise" and by pointing out that these data cooperatives should hold fiduciary obligations to their stakeholders. As such, they can

create value out their members data and ensure good governance and stewardship of data.

Susha, Janssen, and Verhulst [23] proposed a similar kind of actor in the ecosystem of a digital cooperative economy, namely data collaboratives. These are "cross-sector (and public-private) collaboration initiatives aimed at data collection, sharing, or processing for the purpose of addressing a societal challenge" [23, p. 2691]. They differ mainly from data cooperatives in how they are organized: in data collaboratives matching between byer or supplier "(…) is often defined by what kind of data is on offer, and the incentives and control are low" while in data cooperatives meeting common economic, social, and cultural needs through a jointly owned and democratically controlled enterprise is key.

However, the question should be raised whether a data cooperative or collaborative can function as a representative in balanced process (with representatives of consumers, i.e., data cooperatives or collaboratives, and businesses, governmental actors, academia) in today's data ecology in order to establish acceptable methods for consent on data management actions, see also [24].

Above we introduced the notions of data cooperatives and data collaboratives in the context of PDSs. To acknowledge the socio-technical context, we put forward critical questions on user empowerment, power symmetries and user appropriation, so to reflect on the role of users and society in a PDS-enabled data ecosystem.

B. PDS , privacy & user empowerment

Privacy can, and in our opinion should, be seen as a fundamental right and basic human value. In their seminal article, Warren and Brandeis put forward the right to be left alone or the right to an inviolate personality to assert an individual's privacy [25]. Cohen [26] also underlines the value of privacy and how it affords the development of a critical and playful self. The societal value of privacy cannot be reduced to "a simple matter of individual prerogative" [27, p. 1111]. It is therefore striking how an individual control rhetoric on privacy often prevails [28].

Commercial parties, especially, narrate a control rhetoric with a focus on individual control or access restriction, under the guise of user empowerment [29]. When analyzing the Zuckerberg files (a digital archive of all public utterances of Facebook's founder and CEO, Mark Zuckerberg) [29, p. 214] noticed how "Zuckerberg creates a kind of cosmology that places the users, commercial actors, and Facebook shoulder to shoulder – a view that flattens and obfuscates the incomprehensibly major differences in power between these different players.". Using a language that describes users as empowered is in stark contrast with how they have little meaningful options to control their data and information flows [30]. Indeed, as the popular phrasing goes 'users are often considered the product being sold rather than the customer'. In addition, and building further on this metaphor, we would like to add how we barely have any agency on how we are 'packaged' and 'sold'. In this light, PDSs could then be seen as valuable alternatives that put users in the driver's seat. Yet, it should be noted how privacy can still be perceived as a 'control responsibility', defined by [28, p. 5518] as an individual responsibility that can be controlled and needs to be learned by users. Hence, if we want PDSs to be empowering it is still important to treat privacy as a fundamental right. If not, we could merely extend the privacy-as-property logic and further create a false sense of controllability.

'Control' and 'transparency' are often presented as ways to empower end-users in their privacy and data management. Besides an asymmetrical power relationship with service providers and other third parties in which the terms of data extraction are imposed on the users (see infra), it should be noted how users themselves are not always rational in their privacy behaviors. Knijnenburg [31, p. 15], among others, argues to be mindful of the 'control and transparency paradox'. The former refers to how "users claim to want full control over their data, they avoid the hassle of actually exploiting this control.". The latter argues how "privacy notices that are sufficiently detailed to have an impact on people's privacy decisions are often too long, detailed and complex for people to read.". Indeed, there is no guarantee that such behaviors will not unfold when managing data in PDSs. Over the years, privacy scholars have found how terms or services (ToS) or privacy policies are not being read or sufficiently read to be understood [32]–[34]. Nevertheless, we believe that control and transparency can still be empowering when being mindful of current privacy management behaviors and when considering that users are not pure rational agents (cfr. privacy calculus). Considering specific characteristics (e.g., level of privacy or data literacy) as well as data norms where users indicate to what extent they want control over their data or protection, could help to achieve user empowerment.

In the early days of the Internet, scholars and policy makers argued to be mindful of the digital divide. Providing access to ICTs and including vulnerable audiences was considered a priority (e.g., one laptop per child initiative). Later, media scholars argued to also consider the divide in literacy and skills [35]. For vulnerable audiences, the digital divide manifests itself on levels of access, literacy, and skills. Moreover, [36, p. 711] argued how "those who experience most problems online also seem to have the most difficulty obtaining high-quality support even when it is available, creating an even larger 'gap' between those who do and do not need support.". To empower users through PDSs it is important to provide access, literacy, and skills, with specific attention to vulnerable audiences and their needs. Such an approach facilitates empowerment on both an individual and societal level. However, when one does not consider the layerdness of the digital divide and of end-users, implementing PDSs could instigate individual and societal processes of responsibilization creating a new digital divide.

While ensuring privacy and attaining user empowerment through transparency seems difficult when data agency is considered as market agency (making choices in the marketplace from different options for data use), an approach through data cooperatives seems more promising. 'Data cooperatives' as a construct to afford people meaningful agency over their personal data, can mitigate issues related to the 'control rhetoric' (with a focus on individual control or access restriction) and can create an equal playing field where everyone has the same possibilities. Data cooperatives or collaboratives can function as a representative in a balanced process supporting individual users in matching their data with potential data providers, in maintaining control over their data and its unforeseen uses and in aligning

incentives of data providers with their goals, thus ensuring (data) empowerment.

C. PDS & power symmetry

One of the defining characteristics of data capitalism is the persistence of so-called 'data-opolies,' which [37, p. 275] describes as 'companies that control a key platform, which, like a coral reef, attracts users, sellers, advertisers, software developers, apps and accessory makers to its ecosystem". This informational capitalism is centered upon extracting, processing, and using personal data as raw material, which becomes the primary source of monetization and financial value [38]. Through their strategic position as a digital gatekeeper enabling other actors to interact, data-opolies such as Google, Apple and Facebook can extract and exploit a substantial volume and variety of personal data. This ability to commoditize data helps these platforms to build significant market power and results in an uneven distribution of power that is "weighted toward the actors who have access and the capability to make sense of data" [39, p. 23].

While users are locked in closed ecosystems, portability of personal data is almost impossible because platforms are incompatible with one another. As a result, big platforms benefit from network effects enabling them to extract an unprecedented amount of data. This allows leading platforms to obtain more fine-grained profiles of their users, train algorithms more effectively and build a competitive advantage. Although the market power of data-opolies is seldom translated into higher consumer prices, this excessive accumulation of data is not harmless. According to [37], data-opolies raise serious concerns in terms of less privacy, a transfer of wealth from users to platforms, degraded quality, less innovation and rivalry, and political, social, and moral concerns.

Many decentralization evangelists believe that decentralization, or any form of non-hierarchical form of organization, will abolish existing power structures within society and change current data-opolies into an equal playing field where everyone has the same possibilities to extract personal data [40]. The rationale for this belief lies in the idea that decentralization will give organizations an equal chance to deploy PDSs and gather users' data, once they have the user's permission.

For small organizations, decentralization may provide new opportunities to have access to users' personal data that is gathered by other large players such as Facebook and Google. However, several authors have already argued that decentralization does not necessarily imply decentralizing power, see e.g., [40], [41]. In particular, as [40] explain, decentralized systems might comprise a distributed network of nodes, while producing highly centralised effects in terms of wealth or other resources, system information and power asymmetries. Decentralization of personal data storage can shift the competition between organizations to other parts of the data life cycle, namely the phase of developing and managing PDS. Here, companies with more resources will be able to develop more innovative PDS with better performances than those of small companies. As such, their PDS services will likely attract more users, which gives them more power over the conditions under which companies can have access to the users' PDS.

PDSs posit that users cannot reap enough of the current benefits, and this is where they attempt to intervene in the value creation of surveillance capitalism. They propose reorienting markets in order to change who benefits from datafication. Markets or data ecologies shaped by PDSs are to be consumer driven, and the user needs to decide how, and under which terms his/her data are used. PDSs are based on changing the structure of data flows in the data industry. They aim not only at transparency of data flows but at changing who gets to decide about them.

However, the extent to which these changes can be ensured/enforced by individual PDS users seems small. Again, data cooperatives or collaboratives could play a key role in this context. They can create value out their members data and can ensure good governance and stewardship of data for the collective of their users. For example, they could function as an intermediary third party between users and companies, setting up balanced data management processes as well as establishing acceptable methods for consent..

D. PDS & (user) appropriation

Next to questions about user empowerment and power symmetries that might be attained using PDSs, it is also important to reflect on whether people are willing and able to use personal information management systems or personal data stores. In this context, the long-researched 'digital divide', which is also a 'data divide' should be considered as it highlights inequalities in access, knowledge, and awareness of PDSs.

From a broader perspective, more insights are needed in what members of the public think about PDSs and other possible data management models. Here, domestication theory, which emerged from a series of studies that sought to understand the appropriation of artifacts in the specific social setting of the home, can provide an interesting framework as the theory focuses on "(…) what users do to and with technologies in order to fit them into their lives, to make them acceptable" [42, p. 4]. Technologies are not just adopted and accepted; they are actively integrated into households' dynamics via individualized domestication pathways. Furthermore, the identification of factors that cause people to accept new technologies has been researched heavily over the past decades [43]–[45] resulting in widely accepted frameworks to predict and explain the adoption of Information Systems such as the Technology Acceptance model (TAM) [46]. TAM asserts that perceived usefulness (PU) and perceived ease of use (PEU) have a determining impact on the intended and actual use of technology.

Research shows for example that technologies that we refer to as 'Privacy Enhancing Technologies' (PETs) are not being adopted by a significant user base because of problems with usability, bootstrapping, and network effects [47]. Preliminary research on PDSs demonstrated that people are not fully convinced that a PDS would address all their anxieties and that they have concerns about the PDS in terms of its time-consuming character and potential security issues; "(…) PDS did not allay concerns about unnamed others accessing personal data; most participants were skeptical about this data management model." [9, p. 827]. In short, people consider PDS as potentially burdensome, similar to reading the terms of service of digital platforms and consenting to these. As such, PDSs that overly rely on the idea of an autonomous individual or rational economic agent

that is willing and able to participate, might need to be revised.

Also, while PDSs and decentralization promises organizations to make more data available for the services they provide, the question remains whether this influx of additional user data can make a significant contribution to the service that a company provides. Can historical data on a person's purchasing behavior (e.g., PayPal) or the walking routes he/she takes (e.g., Strava) also be used effectively to improve, for example news or video recommendations? In other words: does the idea of 'the more data, the better' always apply? And, more importantly, is it also in proportion to the extent to which the system is being improved? At the very least, it increases the pressure to build more transparency into the UX of personal data stores and recommendation systems so that users gain more insight into the added value that certain data streams can generate.

III. Discussion and conclusion

In this article we have tried to outline (and shape) current discussions on the role and potential of PDS-technologies by eliciting the role of users and society in such PDS driven data ecologies. We have highlighted critical questions on user privacy and empowerment, on power symmetries and on user appropriation using a socio-technical approach.

With regards to user appropriation, we noted that, although PDSs have the potential to give individual users more control, preliminary research shows that individual responsibility for these users was not desirable, because it was perceived as time-consuming. PDSs also might put too much focus on the individual and not enough focus on the business models (or other incentives for data processing). As such, policymakers should be aware of the consequences of treating personal data as an economic object. Afterall, the appropriation of user's personal data is generally not the failure of individuals to exercise control over that data but is caused by surveillance-supported business models that demand that data. In short, conditions of the current data market are not conducive to users securing and exerting market power. Furthermore, to ensure that socially unequal populations are not disadvantaged by data-driven systems, collective data management models like data commons or data cooperatives [48] may be more effective than personalised alternatives.

In terms of power (a)symmetries in the current data ecology, PDSs can reorient markets and change who benefits from datafication, creating not only transparency of data flows but also changing who gets to decide about them. The extent to which these changes can be ensured/enforced by individual PDS users, however, seems small. Data cooperatives, as an intermediary third party between users and companies, can mitigate this by setting up data management processes and methods for consent.

With regards to user empowerment, it became clear that if we want PDSs to be empowering we need to treat (data) privacy as a fundamental right in order not to merely extend the privacy-as-property logic in a PDS-based data ecology. As such we need to consider people's current privacy management strategies and usage of privacy controls while at the same time ensuring that individual empowerment can lead to societal empowerment.

As argued, data cooperatives can play a significant role in ensuring user privacy and empowerment, power symmetries and user appropriation in a PDS-based data ecology. While data cooperatives are definitely not "(…) a one-stop-shop that will fix all the ills of platform capitalism" [22], we see promise in this collective approach to the management of (personal) data as it may reorient markets and change who benefits from datafication.

In this context, future research should not only address the challenges towards realizing a PDS-enabled data ecology (e.g., the need to reconsider the regulatory basis to comply with international data handling standards etc.) but also the potential obstacles or hurdles that hinder the implementation of data cooperatives (e.g., the governance or day-to-day management of these autonomous associations of persons). Here, further research from a socio-technical approach is also needed in order to understand what consumers think about these and other possible data management models.

References

[1] International Telecommunication Union, "Statistics," 2021. [Online]. Available:https://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx.

[2] D. Lupton and M. Michael, "'Depends on who's got the data': Public understandings of personal digital dataveillance," *Surveill. Soc.*, vol. 15, no. 2, pp. 254–268, 2017.

[3] S. Pink, D. Lanzeni, and H. Horst, "Data anxieties: finding trust in everyday digital mess," *Big Data Soc.*, vol. 5, no. 1, p. 2053951718756685, 2018.

[4] J. Vertesi, J. Kaye, S. N. Jarosewski, V. D. Khovanskaya, and J. Song, "Data Narratives: Uncovering tensions in personal data management," in *Proceedings of the 19th ACM conference on Computer-Supported cooperative work & social computing*, 2016, pp. 478–490.

[5] A. Bergström, "Online privacy concerns: A broad approach to understanding the concerns of different groups for different uses," *Comput. Human Behav.*, vol. 53, pp. 419–426, 2015.

[6] S. C. Boerman, S. Kruikemeier, and F. J. Zuiderveen Borgesius, "Exploring motivations for online privacy protection behavior: Insights from panel data," *Communic. Res.*, p. 0093650218800915, 2018.

[7] ComRes and BigBrotherWatch, "UK Public Research – Online Privacy - Big Brother Watch," 2015.

[8] N. A. Draper and J. Turow, "The corporate cultivation of digital resignation," *New Media Soc.*, vol. 21, no. 8, pp. 1824–1839, 2019.

[9] R. Steedman, H. Kennedy, and R. Jones, "Complex ecologies of trust in data practices and data-driven systems," *Information, Commun. Soc.*, vol. 23, no. 6, pp. 817–832, 2020.

[10] H. Choi, J. Park, and Y. Jung, "The role of privacy fatigue in online privacy behavior," *Comput. Human Behav.*, vol. 81, pp. 42–51, 2018.

[11] K. Birch, M. Chiappetta, and A. Artyushina, "The problem of innovation in technoscientific capitalism: data rentiership and the policy implications of turning personal digital data into a private asset," *Policy Stud.*, vol. 41, no. 5, pp. 468–487, 2020.

[12] J. Van Dijck, "Datafication, dataism and dataveillance: Big Data between scientific paradigm and ideology," *Surveill. Soc.*, vol. 12, no. 2, pp. 197–208, 2014.

[13] K. Birch, "Financing technoscience: Finance, assetization and rentiership," in *The Routledge handbook of the political economy of science*, Routledge, 2017, pp. 169–181.

[14] T. Lehtiniemi and J. Haapoja, "Data agency at stake: MyData activism and alternative frames of equal participation," *new media Soc.*, vol. 22, no. 1, pp. 87–104, 2020.

[15] Solid, "SOLID Homepage," 2021. [Online]. Available: https://solidproject.org/.

[16] T. Lehtiniemi, "Personal data spaces: An intervention in surveillance capitalism?," *Surveill. Soc.*, vol. 15, no. 5, pp. 626–639, 2017.

[17] M. Van Kleek and K. OHara, "The future of social is personal: The potential of the personal data store," in *Social Collective Intelligence*, Springer, 2014, pp. 125–158.

[18] C. Füchs, W. Hofkirchner, M. Schafranek, C. Raffl, M. Sandoval, and R. Bichler, "The evolution of the web. From web 1.0 towards web 2.0 and web 3.0," *Int. J. Internet Sci.*, vol. 3, no. 1, 2008.

[19] J. Gelhaar, T. Groß, and B. Otto, "A Taxonomy for Data

Ecosystems," in *Proceedings of the 54th Hawaii International Conference on System Sciences*, 2021, p. 6113.
[20] D. De Bot and T. Haegemans, "Data Sharing Patterns as a Tool to Tackle Legal Considerations about Data Reuse with Solid: Theory and Applications in Europe," 2021.
[21] A. L. Institute, "Exploring legal mechanisms for data stewardship," 2021.
[22] T. Scholz and I. Calzada, "Data Cooperatives for Pandemic Times," *Public Seminar*, 2021. [Online]. Available: https://publicseminar.org/essays/data-cooperatives-for-pandemic-times/.
[23] I. Susha, M. Janssen, and S. Verhulst, "Data collaboratives as 'bazaars'? A review of coordination problems and mechanisms to match demand for data with supply," *Transform. Gov. People, Process Policy*, 2017.
[24] R. Gellman, "Is there a role for consent in privacy?," *IAPP*, 2021. [Online]. Available: https://iapp.org/news/a/is-there-a-role-for-consent-in-privacy/.
[25] Z. Papacharissi, "Privacy as a luxury commodity," *First Monday*, vol. 15, no. 8, 2010.
[26] J. E. Cohen, "What privacy is for," *Harv. L. Rev.*, vol. 126, p. 1904, 2012.
[27] D. J. Solove, "Conceptualizing privacy," *Calif. Law Rev.*, vol. 90, pp. 1087–1156, 2002.
[28] R. De Wolf and S. Joye, "Control responsibility": A critical discourse analysis of Flemish newspapers on privacy, teens and Facebook," *Int. J. Commun.*, vol. 13, pp. 5505–5524, 2019.
[29] A. L. Hoffmann, N. Proferes, and M. Zimmer, "'Making the world more open and connected': Mark Zuckerberg and the discursive construction of Facebook and its users," *New Media Soc.*, vol. 20, no. 1, pp. 199–218, 2018.
[30] M. Willson and T. Leaver, "Zynga's FarmVille, social games, and the ethics of big data mining," *Commun. Res. Pract.*, vol. 1, no. 2, pp. 147–158, 2015.
[31] B. P. Knijnenburg, *A user-tailored approach to privacy decision support*. University of California, Irvine, 2015.
[32] B. Berendt, O. Günther, and S. Spiekermann, "Privacy in e-commerce: Stated preferences versus actual behavior," *Commun. ACM*, vol. 48, no. 4, pp. 101–106, 2005.
[33] J. A. Obar and A. Oeldorf-Hirsch, "The biggest lie on the internet: Ignoring the privacy policies and terms of service policies of social networking services," *Information, Commun. Soc.*, vol. 23, no. 1, pp. 128–147, 2020.
[34] P. G. Kelley, L. Cesca, J. Bresee, and L. F. Cranor, "Standardizing privacy notices: an online study of the nutrition label approach," in *Proceedings of the SIGCHI Conference on Human factors in Computing Systems*, 2010, pp. 1573–1582.
[35] J. Van Dijk, *The deepening divide: inequality in the information society*. Thousand Oaks: Sage, 2005.
[36] E. J. Helsper and A. J. A. M. Van Deursen, "Do the rich get digitally richer? Quantity and quality of support for digital engagement," *Information, Commun. Soc.*, vol. 20, no. 5, pp. 700–714, 2017.
[37] M. E. Stucke, "Should we be concerned about data-opolies?," *Geo. L. Tech. Rev.*, vol. 2, p. 275, 2017.
[38] N. Srnicek, *Platform capitalism*. John Wiley & Sons, 2017.
[39] S. M. West, "Data capitalism: Redefining the logics of surveillance and privacy," *Bus. Soc.*, vol. 58, no. 1, pp. 20–41, 2019.
[40] B. Bodó, J. K. Brekke, and J.-H. Hoepman, "Decentralisation: a multidisciplinary perspective," *Internet Policy Rev.*, vol. 10, no. 2, 2021.
[41] H. Janssen, J. Cobbe, and J. Singh, "Personal information management systems: a user-centric privacy utopia?," *Internet Policy Rev.*, vol. 9, no. 4, 2020.
[42] L. Haddon, E. Mante, B. Sapio, K.-H. Kommonen, L. Fortunati, and A. A. Kant, *Everyday innovators: Researching the role for users in shaping ICT's*. Dordrecht: Springer, 2005.
[43] P. G. W. Keen, "Information systems and organizational change," *Commun. ACM*, vol. 24, no. 1, pp. 24–33, 1981.
[44] V. Venkatesh, M. G. Morris, G. B. Davis, and F. D. David, "User acceptance of information technology. Toward a unified view," *IS Q.*, vol. 27, no. 3, pp. 425–478, 2003.
[45] W. R. King and J. He, "A meta-analysis of the technology acceptance model," *Inf. Manag.*, vol. 43, pp. 740–755, 2006.
[46] F. D. Davis, "A technology acceptance model for empirically testing new end-user information systems: Theory and results." Massachusetts Institute of Technology, 1985.
[47] S. Gürses and C. Diaz, "Two tales of privacy in online social networks," *IEEE Secur. Priv.*, vol. 11, no. 3, pp. 29–37, 2013.
[48] ODI, "Huge appetite for data trusts, according to new ODI research," *ODI*, 2019. [Online]. Available: https://theodi.org/article/huge-appetite-for-data-trusts-according-tonew-odi-research.