Personal information management systems: a user-centric privacy utopia?

Janssen, H.; Cobbe, J.; Singh, J.

DOI
10.14763/2020.4.1536

Publication date
2020

Document Version
Final published version

Published in
Internet Policy Review

INTERNET POLICY REVIEW
Journal on internet regulation

Volume 9 | **Issue** 4

RESEARCH ARTICLE

OPEN ACCESS

PEER REVIEWED

Personal information management systems: a user-centric privacy utopia?

Heleen Janssen *University of Cambridge***Jennifer Cobbe** *University of Cambridge*
Jatinder Singh *University of Cambridge*

DOI: https://doi.org/10.14763/2020.4.1536

Published: 18 December 2020
Received: 1 August 2020 **Accepted:** 30 October 2020

Funding: We acknowledge the financial support of the UK Engineering and Physical Sciences Research Council (EPSRC) [EP/P024394/1, EP/R033501/1], the University of Cambridge (through the Cambridge Trust & Technology Initiative), and Microsoft (through the Microsoft Cloud Computing Research Centre).
Competing Interests: The author has declared that no competing interests exist that have influenced the text.

Citation: Janssen, H. & Cobbe, J. & Singh, J. (2020). Personal information management systems: a user-centric privacy utopia?. *Internet Policy Review*, *9*(4). https://doi.org/10.14763/2020.4.1536

Keywords: Personal data stores, Decentralisation, User empowerment, General Data Protection Regulation

Abstract: Personal information management systems (PIMS) aka personal data stores (PDSs) represent an emerging class of technology that seeks to empower individuals regarding their data. Presented as an alternative to current 'centralised' data processing approaches, whereby user data is (rather opaquely) collected and processed by organisations, PDSs provide users with technical mechanisms for aggregating and managing their own data, determining when and with whom their data is shared, and the computation that may occur over that data. Though arguments for decentralisation may be appealing, there are questions regarding the extent to which PDSs actually address data processing concerns. This paper explores these questions from the perspective of PDS users. Specifically, we focus on data protection, including how PDSs relate to rights and the legal bases for processing, as well as how PDSs affect the information asymmetries and surveillance practices inherent online. We show that, despite the purported benefits of PDSs, many of the systemic issues of online/data ecosystems remain.

1. Introduction

Online systems and services are driven by data. There are growing concerns regarding the scale of collection, computation and sharing of personal data, the lack of user control, individuals' rights, and generally, who reaps the benefits of data processing (German Data Ethics Commission, 2019).

Currently, data processing largely entails the capture of individuals' data by organisations, who use this data for various purposes, in a manner that is often opaque to those to whom the data relates. This general lack of transparency has meant that consent and other legal arrangements for the safe and responsible processing of personal data are considered rather ineffective (Blume, 2012; Cate & Mayer-Schönberger, 2013; Tolmie et al., 2016; German Data Ethics Commission, 2020).

Privacy Enhancing Technologies (PETs) are technologies that aim to help in addressing privacy concerns (The Royal Society, 2019). *Personal data stores* (PDSs), otherwise known as *personal information management systems* (PIMS), represent one class of such technology, focused on data management. In essence, a PDS equips an individual (user) with a technical system for managing their data (a 'device'). Generally, a PDS device provides the user with technical means for mediating, monitoring and controlling: (i) the data captured, stored, passing through, or otherwise managed by their device; (ii) the computation that occurs over that data; and (iii) how and when the data, including the results of computation, is transferred externally (e.g., off-device, to third-parties).

Proponents of PDSs argue that it empowers users, by "put[ting] individuals in control of their data" (Crabtree et al., 2018). This is because PDSs provide means for 'users to decide' what happens to their data; in principle, third-parties cannot access, receive or analyse the data from a PDS without some user agreement or action. In this way, PDSs purport a range of user benefits, from increased privacy and the ability to 'transact' (or otherwise monetise) their data, to better positioning users to gain insights from their own data (see subsection 2.3).

More broadly, PDSs seek to provide an alternative to today's predominant form of data processing, where organisations collect, store and/or use the data of many individuals. As this often occurs within a single organisation's technical infrastructure, there may be limited scope for individuals to uncover – let alone control – what happens with their data. The vision for PDSs is to decentralise data and compute, away from organisations, such that it happens with more user control.

PDS technology is nascent, but growing in prominence. Exemplar PDS platforms currently at various stages of development and availability include Hub of All Things & Dataswift (Dataswift) [1]; Mydex, CitizenMe, Databox and Inrupt/Solid (Inrupt) [2] (which is led by Sir Tim Berners-Lee). As nascent technology, PDSs raise several areas for investigation by academia, policymakers, and industry alike. There is already work, for instance, on how PDSs might facilitate better accountability (Crabtree, 2018; Urquhart, 2019), and on the legal uncertainties surrounding the technology, particularly concerning data protection (Janssen et al., 2020; Chen et al., 2020).

This paper takes a broader view, questioning the extent to which PDS technology can actually empower individuals and address the concerns inherent in data processing ecosystems. After giving an overview of the technology, and its purported benefits in section 2, we examine, in section 3, some data protection implications of PDSs focusing on the user's perspective: whether they support particular legal bases for processing personal data; the social nature of personal data captured by PDSs; and the relation of PDSs to data subject rights. In section 4, we argue that the broader information and power asymmetries inherent in current online ecosystems remain largely unchallenged by PDSs. Section 5 synthesises the discussion, indicating that many of the concerns regarding personal data are systemic, resulting from current data surveillance practices, and concluding that PDSs – as a measure that ultimately still requires individuals to 'self-manage' their privacy – only go so far. [3]

2. Technology overview

PDSs represent a class of data management technologies that seek to localise data capture, storage and the computation over that data towards the individual. Generally, they entail equipping a user with their own device for managing their data. A device operates as a (conceptual) data 'container', in a non-technical sense of the word: a strictly managed technical environment in which data can be captured or

1. Note that Hub-of All-Things (HAT) recently changed its name into Dataswift Ltd; Dataswift Ltd represents the commercial enterprise that grew from the university-led HAT research project which was tasked to build the decentralised HAT infrastructure and the governance model. Where we refer in the text to Dataswift, both the HAT project and the commercial enterprise Dataswift are considered within our analysis.
2. Note that Solid offers the technical infrastructure, while Inrupt is the company offering services that are built on that infrastructure. Where we refer to Inrupt, both the technical infrastructure and the company services come within our analysis.
3. This article builds on our earlier comparative analysis of commercial PDS offerings and different PDS formulations, as focused on data protection concerns (Janssen et al., 2020).

stored or can pass through, and within which certain computation can occur. [4] Some devices are wholly virtual (e.g. Digi.me), hosted in the cloud, while others encompass particular physical equipment such as a box or hub (see e.g. Databox).

PDSs generally purport to empower users through their devices. Though offerings vary, generally PDSs provide technical functionality for:

1. *Local (within-device) capture and storage of user data*. Mechanisms for users to populate their PDS with data from a range of sources, which may include from their phones, wearables, online services, manual data entry, sensors, etc.
2. *Local (on-device) computation*. Enabling computation to occur (software to execute) on the device, which generally entails some processing of data residing with the device.
3. *Mediated data transfers*. Allowing control over the data transferred externally (off-device); including 'raw' user data, the results of computation, and other external interactions (e.g. calls to remote services).
4. *Transparency and control measures*. Tooling for monitoring, configuring and managing the above. This includes governance measures for users to set preferences and constraints over data capture, transfer and processing; visualising and alerting of specific happenings within the device; etc.

The device's technical environment (infrastructure) manages security aspects. This can include data encryption, managing and controlling user access to the device and its data, and providing means for isolating data and compute. Further, it also works to ensure adherence with any policies, preferences and constraints that are set (see #4 above). For instance, if a user specifies that particular data cannot be transferred to some party (or component), or should not be included in some computation, the device's technical environment will ensure these constraints are respected.

Core to many PDSs is allowing for computation (potentially any form of code execution, including analytics) to be 'brought' to the data. This occurs through an *app*: software that executes on a user's device for processing that device's data. [5] Some apps may provide the user with functionality without any external transfer of data. Though often apps will transfer some data off-device (such as the results of com-

4. Note that a 'device' is conceptual, and can be underpinned by a range of technical architectures. In describing the data and processing 'within' a device, we refer to that logically governed by the device. This means, for example, that the data and compute might not necessarily occur all within a single technical component, but could potentially occur in various locations, e.g. across a range of (managed) cloud services.

5. Note that the terminology varies by platform; not all platforms would describe processing as occurring through apps, though generally there is some conceptually similar construct.

putation). PDS proponents describe such functionality as of key industry interest, arguing that receiving only the results of computation (e.g. aggregated findings) avoids the sensitivities, overheads and resistance associated with receiving and managing granular and specific user data (see subsection 2.4). Apps operate subject to constraints: they must define what data sources they seek, the data they transfer, and other details; and users may put constraints on how apps behave, e.g. regarding the data that apps may access, process, and transfer. The device's technical environment ensures adherence to these constraints. Legal mechanisms also operate to govern the behaviour and operation of PDS ecosystems (see subsection 2.2). [6]

2.1 A multi-actor ecosystem

It is worth recognising that there are several actors within a PDS ecosystem. We now introduce those most pertinent for this discussion. The focus is on users, but this article is about empowerment and power, so other actors need to be introduced.

Users are those individuals who hold a device, leveraging the PDS functionality to manage their data.

Organisations are those interested in processing user data. Here, we describe organisations as ***app developers***, as they build apps that process user data for installation on user devices. Again, apps will often transfer some data to the organisation, such as the results of computation. PDSs may also support the transfer of data to an organisation without a specific app. This process is managed through the direct data transfer mechanisms provided by the device (which may itself be a form of app, packaged with the device).

Platforms are the organisations that provide the PDS and/or manage the PDS ecosystem. There will be a range of platforms that differ in their offerings. Often a platform's core offering is equipping a user with a device; though this could vary from merely providing the codebase for users to compile and self-manage the operation of their devices, to providing the entire operational infrastructure—perhaps including hardware, managed cloud services for backup, and so forth (Janssen et al., 2020). Moreover, some platforms envisage hosting 'app stores' or 'data marketplaces' that broker between users and the organisations seeking to process their

6. Note that despite the similar terms (devices, apps, app stores), PDS differ from mobile ecosystems, in that PDSs are governance oriented, with far richer and granular controls. Moreover, the degree of resemblance will depend on the specific formulation of the PDS and its ecosystem – many different approaches are possible.

data, while many platforms require adherence with 'best practices', have defined terms of service, and may even have contractual agreements with users and organisations. In this way, platforms vary in their level of involvement in the operation of the PDS ecosystem.

2.2 Governance regimes

In addition to technical aspects, PDS platforms often entail legal governance mechanisms. These operate to help ensure that app behaviour, and data usage more generally, is compliant with user preferences, and platform requirements. Some of these are encapsulated in a platform's Terms of Service (ToS), which commonly define how the platform can be used, and the platform's position on the allocation of responsibilities and liabilities. Platform ToS often require app developers to have appropriate measures in place to safeguard users against unlawful processing (e.g. Dataswift's acceptable use policy), and to safeguard users against accidental data loss or destruction (idem) while requiring them to, for instance, safely keep their passwords or to regularly update their PDSs for security purposes (e.g. Dataswift's terms for users). Platforms may also have contracts with app developers, which contain business specific terms and conditions, governing their interactions with user data, the functionality of their apps etc. ToS and contracts might stipulate, for example, that app developers must fully comply with platform policies and principles regarding user data processing, where failure to do so may result in the platform terminating their data processing activities (example from Mydex ToS).

2.3 Purported user benefits

PDSs generally purport to provide functionality to empower users. Some claimed benefits for users include:

- Users having granular control over the data captured about them, and how that data is shared and used (Article 29 Data Protection Working Party 2014; Crabtree et al., 2018; Urquhart et al., 2019);
- Better protecting personal data (including 'sensitive' personal data) from access by third parties, by way of the technical functionality provided (Crabtree et al., 2018; Lodge et al., 2018);
- Better informed user consent, by giving more information about data processing. This may be through various means, including the device's monitoring functionality; the app's data usage specifications; platform features, such as app stores ranking and describing app data usage, requiring transparency best practices, etc. (Mydata);
- Compartmentalised data storage and computation to prevent apps from

interacting with data (and other apps) inappropriately, inadvertently and without user agreement/intervention (e.g. Crabtree et al., 2018);
- Providing opportunities for users to gain more insights from their data (e.g., Mydex; Mydata);
- Allowing users to transact with or monetise their personal data (Ng & Haddadi, 2018);
- Generally incentivising developers towards more privacy friendly approaches (Crabtree et al., 2018).

PDSs have also caught the attention of policymakers; the European Commission recently expressed that PDSs and similar tools have significant potential as *"they will create greater oversight and transparency for individuals over the processing of their data [...] a supportive environment to foster [their] development is necessary to realise [their] benefits"* (European Commission, 2020). This potentially indicates that the European Commission might in the future define policy encouraging the development of these tools.

2.4 Purported organisational benefits

For organisations (app developers), the appeal of PDSs is the promise of access to more data—potentially in terms of volume, richness, velocity and variety—for processing. PDS enthusiasts argue that if users better understand how their data is being processed, and feel empowered by way of PDS's control mechanisms, they may be less 'resistant' and harbour a greater 'willingness' for (managed) data sharing and processing (e.g., Control-Shift; Mydata; Digi.me; CitizenMe mention this in their descriptions). Similarly, given that PDSs will encapsulate a variety of user information, PDSs might offer app developers access to a broader range of data types than if they attempted to collect the data themselves (Mydata).

Though PDSs are typically described with reference to an individual, most aim to support *'collective computation'*, whereby the processing of data across many users or (particular) populations is enabled through apps operating on their devices (e.g., Mydata; Databox; CitizenMe; Digi.me). [7] Collective computations often entail some user or population profiling to support various organisational aims—customer insight, market research, details of product usage, or indeed, and as is common in online services to support a surveillance-driven advertising business model (as discussed in section 5). In this way, PDS platforms effectively provide a personal data processing architecture that operates at scale across a population. This is attrac-

7. We use 'collective computation' simply to refer to computation that occurs across a range of user devices. There is potential for the methods facilitating such computation to employ privacy-enhancing mechanisms (e.g. The Royal Society, 2019).

tive for organisations, as PDS platforms with large user-bases offer access to a wider population and thus more data than the organisation would otherwise themselves have access to. Importantly, this also comes without the costs, risks, and compliance overheads incurred in undertaking data collection, storage, and management 'in-house', using their own infrastructure (Crabtree et al., 2018).

2.5 PDS platforms: the commercial landscape

Some predict that PDSs could generate substantial economic benefits for businesses and consumers alike (Control-Shift; Brochot et al., 2015; European Commission, 2020). Although the business models for organisations are likely similar to those already existing, the business models for the *PDS platforms* are unclear and remain under development (Bolychevsky & Worthington, 2018). A range of possible revenue streams for PDS platforms have been developed and proposed. These include:

- Platforms charging organisations fees for access to the PDS ecosystem (e.g., annual fee, Mydex); charges for access to the platform's app store, per user download of their app, etc);
- Platforms charging organisations per 'data transaction' with a PDS device, where the type of transaction (access, computation, and/or transfer of data, including raw data, see e.g. Mydex) and/or the type of data requested (e.g. queries, behavioural data) often determines the price (see e.g. CitizenMe);
- Organisations sharing revenue with the platform through in-app purchases (e.g. Digi.me);
- Platforms charging organisations for support services (e.g. Mydex);
- Users paying a subscription fee, or to unlock additional functionality (Digi.me);
- Platforms selling, renting or leasing PDS devices to users, which could include service or maintenance contracts (Crabtree et al., 2018); or
- Platforms in the public interest (e.g. PDSs platforms for public health) might be 'fee-free', funded through, e.g. donations, and public funds (see e.g. BBC-Box).

As PDSs are a developing area, the business models of platforms are nascent. In practice, one expects that platforms will likely employ a range of monetisation mechanisms.

3. Data protection

A key aim of PDSs is to give users greater visibility and control over the processing of their personal data. PDS architectures concern issues regarding personal data, and therefore the General Data Protection Regulation (GDPR) must be considered.

GDPR centres around three legal roles: *controllers* (acting alone or with others together as joint controllers; (Arts. 4(7), 26 GDPR), *processors* (including sub-processors; Arts. 4(8), 28(4) GDPR), and *data subjects* (Art. 4(1) GDPR). The role of a particular actor as a controller or processor is generally a question of their factual influence over data processing; how an actor describes their role (for example in contract) may be indicative, but won't be definitive (Article 29 Working Party, 2010).

GDPR tasks both controllers and processors with a range of responsibilities and obligations, the bulk of which fall on controllers, given their role in determining the nature of the data processing. Obligations for controllers include complying with data protection principles (Art. 5(1) GDPR), that this compliance is demonstrable (Art. 5(2) GDPR), that their processing of personal data is predicated on one of the GDPR's lawful grounds (Art. 6(1) GDPR), to name a few. Typical rights afforded to data subjects (i.e. those whose personal data is being processed) which controllers are tasked with meeting, include the rights to object to data processing, to have their data erased, or to port data (subsection 3.3).

While PDS technologies and their governance models are still developing, many unresolved data protection issues exist. The assignment of roles and responsibilities in PDS systems is complex, given such ecosystems are largely shaped by the collaboration of multiple parties, including the key actors mentioned here. This reality can be difficult to reconcile with GDPR's approach with controllers who 'orchestrate' the data processing in an entire system. In practice, a PDS's ecosystem can take a number of forms, and the legal position of those involved will depend on the circumstances. Issues of roles and responsibilities under the GDPR in different PDS contexts are explored in detail by Chen et al., and Janssen et al. (2020). In this paper, we consider three key *'user-facing'* data protection considerations: (1) how PDSs, in being oriented towards consent, relates to GDPR's lawful grounds; (2) how personal data often relates to more persons than just the PDS user; and (3) the relationship between PDSs and data subject rights.

3.1 Lawful grounds for processing

GDPR requires that processing is predicated on one of its lawful bases as defined by Art. 6(1) GDPR. Controllers must determine which lawful ground is most appropriate in a given situation, depending on specific purposes and contexts for use, the nature of parties involved, and their motivations and relationships, and of course, the requirements for the lawful basis on which they rely. However, due to the ePrivacy Directive, where the PDS entails a physical (hardware) device, consent will generally be required for app developers to process *any* data (Art. 5(3) ePrivacy

Directive; Janssen et al., 2020). In this context, for such devices the only available basis for processing on these devices will be consent (Arts. 6(1)(a) & 7 GDPR; Recitals 32, 42, 43 GDPR) and explicit consent (for special category data—particular classes of data deemed to require extra protections (Art. 9(1), Recitals 51-56 GDPR)). For 'virtual' PDS devices, such as those cloud hosted (as are currently by far the most common), legal bases other than consent may be available (unless that data is special category data, in which case explicit consent is often the only option).

PDS devices are fundamentally oriented towards supporting the grounds of (user) consent and contract (where the processing is necessary for the performance of a contract to which the user is a party) as the legal bases for processing. Importantly, both consent and contract are grounds that require agreement by the data subject to render the processing lawful. PDS platforms are generally explicitly designed for supporting such, by requiring active user agreement regarding data processing (Crabtree et al., 2018; Urquhart 2019). PDSs generally purport functionality that aims at informing users, e.g. providing them information about an app and its related data processing, and requiring the user to take positive actions, e.g. agreeing to terms upon installing the app, configuring data usage preferences and policies, in order for that processing to occur.

There are also lawful grounds for processing, such as legal obligation, public interest or legitimate interest which allow *the controllers*—not the data subjects (users)—to decide whether processing can occur. That is, user consent is not required for certain public tasks (e.g. perhaps in taxation), or for legitimate controller interest (e.g. perhaps for the processing of certain data to detect fraud). The requirements vary by legal basis, and can include (depending on the ground) considerations like the necessity of that processing (Arts. 6(1)(b)—(f) GDPR), that controller interests are balanced with the fundamental rights of the data subject (Art. 6(1)(f) GDPR; Kamara & De Hert, 2018), and a foundation in compatible member state law (Arts. 6(1)(c) and (e) GDPR). These grounds for processing that are *not* based on specific and active user involvement or agreement are rarely considered in PDS architectures, and at present it is unclear how PDS architectures would support or reconcile with these grounds where they may apply (Janssen et al., 2020).

3.2 Social nature of personal data

Personal data is relational and social by nature; it often does not belong to one single individual, as much personal data is created through interactions with other people or services (Article 29 Working Party, 2017; Crabtree & Mortier, 2015).

In practice, a PDS device will likely capture data relating to multiple individuals other than the user—for example, through sensing data from other dwellers or visitors in and around someone's home. This raises interesting questions regarding the mechanisms for one to control what is captured about them in someone else's PDS. That is, there may be conflicting visions and preferences between the user and others regarding the use and processing of 'joint' data, and these others may also have data subject rights (see subsection 3.3). At present, PDSs generally give a device's *user* greater control over the processing related to that device; functionality enabling the preferences and rights of *others* to be managed and respected has yet had little consideration. This is an area warranting further attention.

3.3 Supporting data subject rights

GDPR affords data subjects several rights regarding the processing of their personal data. These include the rights of access to their personal data (Art. 15), rectification of inaccurate personal data (Art. 16), erasure (Art. 17), to object (Art. 21), to restrict the processing of their data (Art. 18), to port their data to another controller in a commonly used machine-readable format (Art. 20 GDPR), and to not be subject to solely automated decision-making or profiling which produces legal or similarly significant effects (Art. 22 GDPR). Controllers are tasked with fulfilling these rights. Data subject rights are not absolute—GDPR imposes conditions on the exercise of some rights, and not all rights will apply in every situation.

Data subject rights have had little consideration in a PDS context. Again, to improve the transparency of processing, PDSs usually afford users some visibility over what occurs on-device and provide information on their device's interactions (data exchanges) with organisations (Urquhart et al., 2018). They also generally offer certain controls to manage on-device processing. As such, some have suggested that PDSs may (at least for data within the PDS device) to some extent "negate" a user's need to exercise certain data subject rights (Urquhart et al., 2018), where such mechanisms could potentially provide means for users to themselves restrict certain processing, and erase, delete or port data, and so forth. However, current PDS tooling, at best, only gives certain users visibility and the ability to take action regarding processing happening on-device (see subsection 4.1). Data subject rights, however, are broader, and encompass more than simply giving users visibility over on-device data processing. Users will, for instance, have interests in the behaviour of organisations involved in processing.

GDPR requires controllers to account for data protection considerations, including those relating to rights, in their technological and organisational processes (Data

protection by design, GDPR Art 25(1)). This has implications not only for app developers, but also for PDS platforms, who could provide mechanisms that specifically and more holistically facilitate users in exercising their rights. Though there may be questions as to whether this is legally obliged—for instance in light of the complexities regarding a platform's roles and responsibilities given that Art 25(1) applies to *controllers* (see Chen et al., 2020; Janssen et al., 2020). Indeed, these considerations are exacerbated as some PDSs represent 'open source' projects, potentially involving a wide range of entities in the development, deployment and operation of the platform and/or device functionality. However, regardless of any legal obligation, any PDS platform should aim to better support users with regards to their data rights, given that this is wholly consistent with the stated aims of PDSs as 'empowering users'.

Beyond PDS functionality that specifically aims at rights, there is potential for PDS transparency mechanisms to assist users with their rights more generally. For instance, PDSs might, by providing information, help users in detailing and targeting their rights requests. User observation of, or a notification by the platform indicating particular application behaviour, might encourage users to exercise their right 'to find out more', or perhaps encourage them to validate that their rights requests were properly actioned. This might help users to determine whether processing should continue, or help them confirm whether the information provided by the controller corresponds to the operations observed on-device.

The right to data portability grants users the right to receive copies of the data they provided to a controller in an electronic format, and to transfer that data or to have it transferred to another controller. This can only be invoked if the processing was based on the lawful grounds of consent or contract (Art. 20(1)(a) GDPR), and concerns only that data provided by data subjects themselves (Art. 20 (1) GDPR; Article 29 Working Party, 2016; Urquhart et al., 2017).

Portability is considered a key means for users to 'populate' their PDSs by bringing their data from an organisation's databases to the PDS (Art. 20 GDPR; Article 29 Working Party, 2019). Indeed, some PDS platforms describe the right as enabling users to 'reclaim' their data from organisations (e.g. CitizenMe; Dataswift; Digi.me),and envisage offering users technical mechanisms that leverage portability rights for populating their devices (idem). Subject access requests (Art. 15(3) GDPR) may also assist in populating devices, particularly given they are less constrained in terms of when it can be used, and usually result in more information than would be received from a portability request. However, subject access requests do not require that the data be returned in a machine-readable format. Without agreed-up-

on interoperability standards, using subject access requests (and indeed, even portability requests to some degree) to populate PDSs will often be impractical and cumbersome.

PDSs' transparency mechanisms are also relevant here, as they can work to improve the user's position. This is because such mechanisms can expose the on-device computations, possibly including the results of those computations, and potentially in a meaningful technical format. This is useful not only for portability considerations (e.g. in a PDS context, potentially moving the results of computations across apps), but also in generally providing users with more knowledge and insight into the nature of data processing occurring.

4. Information asymmetries

PDS platforms state that they empower users by providing them with means for increased transparency and control, enabling users to take better, more informed decisions about whether to engage or, indeed, disengage with particular processing. However, systemic information and power asymmetries are inherent in current digital ecosystems, whereby the highly complex and largely opaque nature of data processing amplifies the asymmetries between data subjects and the organisations processing their data (Mantelero, 2014). These asymmetries, stemming from an unequal distribution of opportunities in terms of understanding, knowledge, prediction, risk assessment, and so forth (Mantelero, 2014), make it difficult if not impossible for even knowledgeable users to properly evaluate and come to genuinely informed decisions about the processing of their data (Solove, 2013; Solove, 2020).

The opaque nature of data processing is largely systemic because users of digital services often lack (or are prevented from gaining) knowledge or understanding of: (1) the practices of organisations capturing and processing their data, including the details, reasons for and implications of holding particular data or performing particular computation; (2) the data sharing practices of those organisations with third parties and beyond; (3) the technical details of the systems involved; (4) the data-driven, and indeed, often surveillance-driven business models (see section 5); and (5) the insights and power that organisations can gain through having access to data, particularly where data is aggregated or computation occurs at scale (collective computation). Legal issues may further contribute to systemic problems—including information asymmetries—within digital ecosystems (Cohen, 2019); for example, copyright, trade secrecy, or documents or databases owned by large organisations might work to restrict the information that is available to the public. However, these restrictions are not absolute and do not apply to every

stakeholder. Under certain conditions, courts or regulators can be given access to data relating to trade secrets or databases not generally available to the public (Art. 58(1)(e); Recital 63 GDPR).

Crucially, PDSs only partially respond to these issues and therefore only partially address the systemic nature of the information asymmetries of digital ecosystems. Providing a localised, user-centric containerisation of data and processing may assist users in gaining some knowledge of what happens with their personal information, but only to a limited extent. While users might gain some greater understanding over the data processing relating to their device, PDSs themselves are unlikely to solve these systemic information asymmetries. Fundamentally, PDSs are grounded in the mistaken idea that with enough information presented in the right way, individuals will be able to overcome barriers that are ultimately structural and systemic in nature (Nissenbaum, 2011).

4.1 Organisational data processing practices remain largely opaque

An organisation's intentions, motivations and behaviours may not always be clear to users (Burrell, 2016). Attempting to address this, PDSs require app developers to provide some information about their organisational processes and intentions. Such information (often encapsulated in 'app manifests') might include details of the types of data an app will process; the app developer's purposes for that processing; the risks of the app; or with whom the app developer may share data received from the PDS (Crabtree, 2018; Janssen et al., 2020). [8] However, less discussed in PDS proposals is conveying information about why *that* particular data is necessary (as opposed to other, perhaps less sensitive data), why *these* weights are attached to particular data in the analytics process, and, more broadly, why *that* particular processing needs to occur, and the possible data protection implications this may have. This is an area needing attention.

We now elaborate two additional aspects: *(i)* the lack of information available regarding data that flows beyond organisational boundaries, and *(ii)* how the opacity of app developers' processes can hinder PDS platform's governance processes. Note, however, that even if PDSs could provide additional information on developers' processing practices, the utility of this for users is unclear. Moreover, this risks

8. Note that differences exist as to what PDSs require from app developers to describe in their manifests. Databox envisages to assess risks as to whether an app developer intends to share the data with third parties, while other platforms might not envisage any risk assessment on this aspect (or it is not explicit from their documentation that they do this).

potentially creating a false sense of having adequately informed users while in actuality the problems caused by information asymmetries remain (this dimension is explored in subsection 4.2).

4.1.1 Transparency and control diminish as data moves across boundaries

Once data moves beyond a system or organisation's boundaries, the visibility over that data typically diminishes, as does the ability to control any subsequent processing (Singh et al., 2017; Crabtree et al., 2018; Singh et al., 2019). So, while PDSs might provide users with insights into device-related processing, PDSs generally will not (at least at a technical-level) provide users with information about – let alone access to – data that has moved to app developers (and, indeed, beyond). Even in a PDS context, users will (still) therefore have little meaningful information regarding the specifics of the data actually being shared between organisations and third parties. [9]

The fact that some data usage is essentially out of sight raises various risks, including, for instance, around secondary uses of data that a user would not have agreed with, e.g. undisclosed monetisation (Silverman 2019), or unexpected or undesired inferences or profiling, which could be used to influence, nudge or manipulate (Wachter et al., 2019). Moreover, as many online services entail a 'systems supply-chain' (Cobbe et al., 2020) – whereby services from various organisations are used to deliver functionality – there may be little visibility regarding the specific organisations involved in processing once the data moves 'off-device'.

Though these issues are not typically the focus of PDSs, they relate to the technology's broader aims. PDSs might potentially assist where technical mechanisms can improve the visibility over data processing and transfer from the device to the first recipient (one-hop), and legal means can govern such transfers (subsection 2.2). For instance, Mydex stipulates in its ToS that app developers may not transfer user data that is obtained through the platform's service to third-parties, except to the extent that this is expressly permitted in the relevant app developer notice (see, for another example, Dataswift). Through these measures, PDSs might better inform users of – and offer greater control over – what is *initially* transferred 'off-device'. However, the ability to actually monitor, track and control data as it moves across technical and administrative boundaries is an area for research (e.g. see Singh et al., 2017; Singh et al., 2019; Pearson & Casassa-Mont, 2011).

9. Databox envisages to give indications to users in their risk assessment whether app developers intend to transfer user data beyond the EU (which entails high risks to that data), or whether an app developer transfers personal data to other recipients (this also entails high risks to user data).

4.1.2 Issues with opacity and non-compliance for PDS platforms

Many PDS platforms describe ToS and contractual arrangements with app developers, which define how app developers may process user data. However, organisational data processing opacities can also hinder platforms in uncovering and assessing the risks of non-compliant app and developer behaviour (Crabtree et al., 2018). Platforms' monitoring and compliance measures might to some extent mitigate the implications of limited user understanding of app developers' data processing practices, where non-compliance by a developer could result in termination of their processing, the app's removal from the platform, payment of damages, etc (e.g. ToS of Mydex). This could entail log file analysis, app audits, and manual reviews, including 'sandboxing' (examining behaviour in a test environment), and reporting measures when non-compliance is detected on a device (comparable to software 'crash reports' in other contexts).

However, there are questions around whether platforms themselves can effectively detect or otherwise uncover non-compliance by app developers. Platform operators generally position themselves to not have direct access to user devices (including data, processing and logs thereof), which limits their visibility over what is happening 'on the ground'. Platforms becoming actively involved in device monitoring, by gaining visibility over the happenings on user devices, brings additional data protection considerations, while effectively involving a device 'backdoor' which has security implications and could undermine the PDS ecosystem. Questions of incentives are also raised, e.g. regarding the propensity for a provider to take action against app developers where doing so has impacts on the platform's income or business. These issues need further attention.

4.2. Users still require knowledge and expertise

PDSs are oriented towards data protection concerns, particularly regarding the difficulties in obtaining genuinely informed consent and offering users real control. But for this to be effective, users must also be able to understand the potential data protection implications of processing. This means PDS users will require some degree of data protection expertise and knowledge to enable them to comprehend the implications of certain computation and transfers. Though PDSs seek to provide users with more information about processing, and may offer some general guidance, it will not always be clear to users what the full implications of certain data processing or transfers are—not least given the risks are often contextual. A user might, for instance, allow an app developer to build a detailed profile, not realising these could subsequently be used to influence, nudge or manipulate them-

selves and others (Wachter & Mittelstadt, 2019).

Similarly, an app's or platform's explanations and visualisations of data flows, technical parameters, configuration and preference management mechanisms, and so forth, can also be complex and difficult to understand for non-experts (Anciaux et al., 2019). Moreover, identifying where app behaviour does not comply with user preferences or is unexpected can be challenging even for expert users, let alone the non-tech-savvy. Users will therefore also require some technical expertise and knowledge to meaningfully interrogate, control and interact with the functionality of the platform (Crabtree et al., 2018).

As a result, though PDSs seek to better inform users, simply providing them with more information may not produce substantially better informed and empowered users. That is, the information asymmetries currently inherent in digital ecosystems may remain largely unaddressed, and many users may remain largely unempowered and under-protected.

There is on-going research by the PDS community on how platforms can make their transparency and control measures more effective (Crabtree et al., 2018). Default policies or usage of 'policy templates' might enable third parties (civil society groups, fiduciaries, etc) to set a predefined range of preferences (in line with certain interests and values) which users can easily adopt. Generally, mechanisms facilitating the meaningful communication and management of data protection risks and implications are an important area of research, not just for PDSs, but for digital ecosystems as a whole.

4.3 App developers may still collect and process at scale

Many PDSs seek to support collective computations, allowing app developers to process user data at scale to generate insights from across a population (subsection 2.4). In practice, this likely contributes to further consolidating the information asymmetries between users and organisations. PDSs may help users to understand these asymmetries to some extent, as they allow users to generate insights into the personal data in their own PDSs. However, the fact that app developers can operate across user PDSs—and are encouraged by platforms to do so—means that they can process the data from many users, and thus remain better informed than individual users can ever be. Although an individual's data may be interesting to that individual, it is analysing data at scale that can provide the insights into user behaviour and preferences that are often truly valuable to organisations. It is unlikely that PDSs will address this systemic issue by means of any of their mea-

sures; indeed, by enabling and encouraging collective computations, PDSs are likely to even further contribute to these asymmetries.

As we will explore next, these asymmetries do not only exist with respect to individual users, but also society as a whole. This is because in the current digital environment, power resides with organisations who have the ability to access and process data. In facilitating collective computations, PDSs continue to support organisations to process data at scale.

5. Discussion: PDSs, privacy self-management and surveillance capitalism

A range of commercial business models are surveillance oriented, where economic value is extracted by collecting and analysing extensive data about people's behaviour, preferences, and interests (Andrejevic, 2011; Fuchs, 2011; Palmås, 2011; Zuboff, 2015). At present, this typically involves aggregating individual data, and analysing that aggregated data to identify patterns. The knowledge obtained through that analysis is used for various purposes. In the context of online services, where the issues are particularly pronounced, this includes algorithmically personalisation to keep users engaged with the service and to target advertising (Cobbe & Singh, 2019). Often this involves profiling, which poses threats to personal integrity, and online services often target user vulnerabilities for exploitation with addictive designs, dark patterns, and behavioural nudging (Yeung, 2017). Online service providers can work towards vendor lock-in and systemic consumer exploitation. Given the central commercial and economic imperatives of most online services, nearly all data-driven business models involve (to some degree) the trading of data and insights for profit (German Data Ethics Commission, 2019). Note, however, that not only online service providers are surveillance-oriented; PDSs themselves also encourage traditional off-line business models to be augmented with some form of user surveillance, for example, to observe the nature of product usage in a home. The extensive processing of personal data in surveillance-oriented or supported business models raises a range of concerns (Kerber, 2016; Christl, 2017; Myers West, 2017).

As discussed in section 2, PDSs seek to address these concerns by giving users greater 'control' over their data and its processing through more information and options regarding processing *and* then enforcing their choices (by bringing the data processing closer to the user and placing legal and technical constraints on it). In this way, as discussed in section 3, PDSs adopt an approach to privacy and data protection that is still centred on consent-based grounds for processing, working

to achieving more effective 'notice and consent'. Although the approach taken by PDSs may *seem* to empower users by giving them more 'control', *(i)* the problems with 'notice and consent' as a way of protecting users in digital ecosystems are well-established (Barocas & Nissenbaum, 2009; Sloan & Warner, 2013; Barth & De Jong, 2017; Bietti, 2020), and *(ii)* it does not fundamentally challenge the logic of those business models and surveillance practices. PDSs therefore remain firmly grounded in the logic of 'privacy self-management' (Solove, 2013; Solove, 2020), whereby individuals are expected to manage their own privacy and are themselves held responsible where they fail to adequately do so. This can be understood as part of a broader trend of 'responsibilisation' in Western societies (Hannah-Moffat, 2001; Ericson & Doyle, 2003; Brown, 2015); putting ever more responsibility on individuals to manage risks in various aspects of their lives, despite the existence of systemic issues beyond their control that can make doing so difficult if not impossible (such as the asymmetries described in section 4 that PDSs do not sufficiently alleviate).

Further, PDSs fail to deal with the realities of collective computations, whereby app developers process user data in aggregate and at scale (subsection 2.2), or with the social nature of personal data (subsection 3.3). Collective computations still exist in—indeed, largely result from—the often commercial drivers for PDS platforms and apps. Through these computations PDSs both allow and contribute to further consolidation of power and information asymmetries (subsection 4.3). However, concerns about collective computations go beyond commercial processing, such as where platforms or app developers pursue public policy or security ends (rather than or additional to commercial gains). This is of significant concern, given the rich, detailed and high-personal nature of the information that a PDS device might capture. Moreover, the social nature of personal data means that individual-level controls are sometimes inappropriate (subsection 3.2)—processing may affect a number of people, only one of whom will have had an opportunity to intervene to permit or constrain it. In all, the individualist approach taken by PDSs, rooted firmly in self-management, does not and cannot capture these more collective, social dimensions of privacy and data protection.

The inability of PDSs to adequately address these concerns speaks to a more fundamental issue with PDSs as a concept: they put too much onus on the individual and not enough focus on the business models (or other incentives for data processing). The root cause of the appropriation of user's personal data is generally not, in fact, the failure of individuals to exercise control over that data, but those surveillance-supported business models that demand the data in the first place.

These business models operate at a systemic level, supported by information asymmetries, commercial considerations, legal arrangements (Cohen, 2019), network effects, and other structural factors, and beyond the control of any individual user.

Indeed, the information asymmetries inherent in surveillance business models result in a significant asymmetry of power between users and app developers (Mantelero 2014). As Lyon argues, through information asymmetries, surveillance "usually involves relations of power in which watchers are privileged" (Lyon, 2017, p. 15). This power asymmetry is at the core of how surveillance capitalism attempts to extract monetary value from individuals, by modifying their behaviour in pursuit of commercial interests (Zuboff 2015). Yet, as discussed above, PDSs seek to 'empower' users without significantly dealing with those asymmetries. Nor do they address other systemic factors with structural causes that disempower users in favour of organisations. While PDSs seek to decentralise processing to users' devices, then, it does not follow that power will also be decentralised to users themselves: *decentralising processing does not necessarily imply decentralising power*. Without a more systemic challenge to surveillance-based models for deriving value, shifting away from individualised forms of notice and consent and alleviating the effect of information asymmetries and other structural issues, the underlying power dynamic in those surveillance models—skewed heavily in favour of organisations rather than individuals—remains largely unchanged.

Relevant is what Fuchs describes as a form of academic 'victimisation discourse', where "privacy is strictly conceived as an individual phenomenon that can be protected if users behave in the correct way and do not disclose too much information" (Fuchs, 2011, p. 146), while issues related to the political economy of surveillance capitalism—advertising, capital accumulation, the appropriation of user data for economic ends—are largely ignored or unchallenged. Responses to these business models that are grounded in placing ever-greater responsibility onto users to actively manage their own privacy, in the face of systemic challenges such as endemic surveillance and data monetisation, are destined to fail. This is the case with PDSs as currently envisaged. Indeed, as previously noted, PDSs have even been described as a way of reducing user 'resistance' to data sharing, bringing about a greater 'willingness' to allow personal data to be processed (subsection 2.4). This not only explicitly accepts the logic of these business models, but appears to make them easier to pursue. In this way, PDSs following this approach might lull users into a false sense of security through the rhetoric of greater 'choice', 'control', and 'empowerment'—despite the evidence that these are flawed

concepts in light of the structural and systemic nature of the concerns—while in practice facilitating the very data extraction and monetisation practices that users may be trying to escape.

6. Concluding remarks

PDSs are nascent, but growing in prominence. Their proponents claim that PDSs will empower users to get more from their data, and to protect themselves against privacy harms by providing technical and legal mechanisms to enforce their choices around personal data processing. Though, as we have detailed, their ability to deal with the broader challenges associated with current data processing ecosystems appears limited. Regarding data protection, platforms, regulators and lawyers might together work on the specific data issues brought by PDSs, including how best to deal with issues concerning the rights of data subjects. However, despite any such efforts, and regardless of the purported benefits of PDSs, most of the issues inherent to the systemic information asymmetries and challenges in the current ecosystems remain. While PDSs might offer some helpful user-oriented data management tools, they are fundamentally grounded in the mistaken idea that with enough information presented in the right way, individuals will be able to overcome barriers that are ultimately structural and systemic in nature.

References

Anciaux, N. (2019). Personal Data Management Systems: The security and functionality standpoint. *Information Systems*, *21*, 13 – 35. https://doi.org/10.1016/j.is.2018.09.002

Andrejevic, M. (2011). Surveillance and Alienation in the Online Economy. *Surveillance & Society*, *8*(3), 270 – 287. https://doi.org/10.24908/ss.v8i3.4164

Article 29 Data Protection Working Party. (2007). *Opinion 1/2010 on the concepts of 'controller' and 'processor'. (WP169 of 16 February 2010)*.

Article 29 Data Protection Working Party. (2010). *Opinion 1/2010 on the concepts of 'controller' and 'processor'. (WP169 of 16 February 2010)*.

Article 29 Data Protection Working Party. (2014). *Opinion 8/2014 on Recent Developments on the Internet of Things. (WP 223 of 16 September 2014)*.

Article 29 Data Protection Working Party. (2016). *Guidelines on the right to data portability (WP242 rev.01 13 December 2016)*.

Barocas, S., & Nissenbaum, H. (2009). On Notice: The Trouble with 'Notice and Consent'. *Proceedings of the Engaging Data Forum: The First International Forum on the Application and Management of Personal Electronic Information*.

Barth, S., & De Jong, M. (2017). The privacy paradox – Investigating discrepancies between expressed privacy concerns and actual online behavior – A systematic literature review'. *Telematics and Informatics*, *34*(7), 1038 – 1058. https://doi.org/10.1016/j.tele.2017.04.013

Bietti, E. (2020). Consent as a Free Pass: Platform Power and the Limits of the Informational Turn. *Pace Law Review*, *40*, 317 – 398.

Binns, R. (2020). Human Judgement in Algorithmic Loops: Individual justice and automated decision-making. *Regulation & Governance*, 1 – 15. https://doi.org/10.1111/rego.12358

Blume, P. (2012). The inherent contradictions in data protection law. *International Data Privacy Law*, *2*(1), 26 – 34. https://doi.org/10.1093/idpl/ipr020

Bolychevsky, I., & Worthington, S. (2018, October 8). Are Personal Data Stores about to become the NEXT BIG THING? [Blog post]. *@shevski*. https://medium.com/@shevski/are-personal-data-stores-about-to-become-the-next-big-thing-b767295ed842

Brochot, G. (2015). *Personal Data Stores* [Report]. Cambridge University. https://ec.europa.eu/digital-single-market/en/news/study-personal-data-stores-conducted-cambridge-university-judge-business-school

Brown, W. (2015). *Undoing the Demos: Neoliberalism's Stealth Revolution*. Zone Books.

Burrell, J. (2016). How the machine "thinks": Understanding opacity in machine learning algorithms. *Big Data & Society*, *3*(1), 1–12. https://doi.org/10.1177/2053951715622512

Cate, F. H., & Mayer-Schönberger, V. (2013). Notice and consent in a world of Big data. *International Data Privacy Law*, *3*(2), 67 – 73. https://doi.org/10.1093/idpl/ipt005

Chen, J. (2020). Who is responsible for data processing in smart homes? Reconsidering joint controllership and the household exemption. *International Data Privacy Law*. https://doi.org/10.1093/idpl/ipaa011

Christl, W. (2017). *Corporate Surveillance in Everyday Life* [Report]. Cracked Labs. https://crackedlabs.org/en/corporate-surveillance

Cobbe, J. (2020). What lies beneath: Transparency in online service supply chains. *Journal of Cyber Policy*, *5*(1), 65 – 93. https://doi.org/10.1080/23738871.2020.1745860

Cobbe, J., & Singh, J. (2019). Regulating Recommending: Motivations, Considerations, and Principles. *European Journal of Law and Technology*, *10*(3), 1 – 37. http://ejlt.org/index.php/ejlt/article/view/686

Cohen, J. E. (2019). *Between Truth and Power: The Legal Constructions of Informational Capitalism*. Oxford University Press. https://doi.org/10.1093/oso/9780190246693.001.0001

ControlShift. (2014). *Personal Information Management Services – An analysis of an emerging market: Unleashing the power of trust* [Report]. ControlShift.

Crabtree, A. (2018). Building Accountability into the Internet of Things: The IoT Databox Model. *Journal of Reliable Intelligent Environments*, *4*, 39 – 55. https://doi.org/10.1007/s40860-018-0054-5

Crabtree, Andy, & Mortier, R. (2015). Human Data Interaction: Historical Lessons from Social Studies and CSCW. In N. Boulus-Rødje, G. Ellingsen, T. Bratteteig, M. Aanestad, & P. Bjørn (Eds.), *ECSCW 2015: Proceedings of the 14th European Conference on Computer Supported Cooperative Work, 19-23 September 2015, Oslo, Norway* (pp. 3–21). Springer International Publishing. https://doi.org/10.1007/978-3-319-20499-4_1

Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector. http://data.europa.eu/eli/dir/2002/58/oj

Directive (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of personal data, and repealing Directive 95/46/EC, (2016).

E-Privacy Directive – Directive 2002/58/EC of the European Parliament and the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector, (2002). http://data.europa.eu/eli/dir/2002/58/2009-12-19

Ericson, R. V., & Doyle, A. (2003). *Risk and Morality*. University of Toronto Press.

European Commission. (2020). *A European strategy for Data*. European Union. https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1593073685620&uri=CELEX%3A52020DC0066

European Data Protection Board. (2019). *Opinion 5/2019 on the interplay between the ePrivacy Directive and the GDPR, in particular regarding the competence, tasks and powers of data protection authorities* (Opinion No. 5/2019; pp. 38 – 40). European Data Protection Board.

Fuchs, C. (2011). An Alternative view on the Privacy of Facebook. *Information*, *2*(1), 140 – 165. https://doi.org/10.3390/info2010140

German Data Ethics Commission. (2019). *Gutachten der Deutschen Datenethik Kommission* [Expert opinion]. Datenethikkomission. https://datenethikkommission.de/wp-content/uploads/191015_DEK_Gutachten_screen.pdf

Hannah-Moffat, K. (2001). *Punishment in Disguise: Penal Governance and Canadian Women's Imprisonment*. University of Toronto Press.

Janssen, H., Cobbe, J., Norval, C., & Singh, J. (2020). *Decentralised Data Processing: Personal Data Stores and the GDPR* [Forthcoming]. https://doi.org/10.2139/ssrn.3570895

Janssen, H., Cobbe, J., & Singh, J. (2019). *Personal Data Stores and the GDPR's lawful grounds for processing personal data*. Data for Policy, Kings College London. https://doi.org/10.5281/zenodo.3234880

Kamara, I., & De Hert, P. (2018). *Understanding the balancing act behind the legitimate interest of the controller ground: A pragmatic approach*. (Working Paper No. 4/12; pp. 1 – 33). Brussels Privacy Hub.

Kerber, W. (2016). Digital Markets, data, and privacy: Competition law, consumer law and data protection. *Journal of Intellectual Property Law & Practice*, *11*(11), 855 – 866. https://doi.org/10.1093/jiplp/jpw150

Lodge, T. (2018). Developing GDPR compliant apps for the edge. *Proceedings of the 13th International Workshop on Data Privacy Management*, 313 – 328. https://doi.org/10.1007/978-3-030-00305-0_22

Lyon, D. (2017). *Surveillance Studies: An Overview*. Polity Press.

Mantelero, A. (2014). Social Control, Transparency, and Participation in the Big Data World. *Journal of Internet Law*, 23 – 29. https://staff.polito.it/alessandro.mantelero/JIL_0414_Mantelero.pdf

Myers West, S. (2019). Data Capitalism: Redefining the Logics of Surveillance and Privacy. *Business & Society*, *58*(1), 20–41. https://doi.org/10.1177/0007650317718185

Ng, I., & Haddadi, H. (2018, December 28). Decentralised AI has the potential to upend the online economy. *Wired*. https://www.wired.co.uk/article/decentralised-artificial-intelligence

Nissenbaum, H. (2011). A Contextual Approach to Privacy Online. *Dædalus*, *140*(4), 32–48. https://doi.org/10.1162/DAED_a_00113

Palmås, K. (2011). Predicting What You'll Do Tomorrow: Panspectric Surveillance and the Contemporary Corporation. *Surveillance & Society*, *8*(3), 338 – 354. https://doi.org/10.24908/ss.v8i3.4168

Pearson, S., & Casassa-Mont, M. (2011). Sticky Policies: An Approach for managing Privacy across Multiple Parties. *Computer*, *44*(9), 60 – 68. https://doi.org/10.1109/MC.2011.225

Poikola, A., Kuikkaniemi, K., & Honko, H. (2014). *MyData – A Nordic Model for human-centered personal data management and processing* [White Paper]. Open Knowledge Finland.

Selbst, A. D., & Powles, J. (2017). Meaningful information and the right to explanation. *International Data Privacy Law*, *7*(4), 233 – 243. https://doi.org/10.1093/idpl/ipx022

Silverman, C. (2019, April 14). Popular Apps In Google's Play Store Are Abusing Permissions And Committing Ad Fraud. *Buzzfeed*.

Singh, J. (2017). Big Ideas paper: Policy-driven middleware for a legally-compliant Internet of Things. *Proceedings of the 17th ACM International Middleware Conference*. https://doi.org/10.1145/2988336.2988349

Singh, J. (2019). Decision Provenance: Harnessing Data Flow for Accountable Systems. *IEEE Access*, *7*, 6562 – 6574. https://doi.org/10.1109/ACCESS.2018.2887201

Sloan, R. H., & Warner, R. (2013). *Beyond Notice and Choice: Privacy, Norms, and Consent* (Research Paper No. 2013–16; pp. 1 – 34). Chicago-Kent College of Law. https://doi.org/10.2139/ssrn.2239099

Solove, D. (2013). Privacy Self-Management and the Consent Dilemma. *Harvard Law Review*, *126*, 1888 – 1903. https://harvardlawreview.org/2013/05/introduction-privacy-self-management-and-the-consent-dilemma/

Solove, D. (2020). *February 11. The Myth of the Privacy Paradox* (Research Paper No. 2020–10; Law School Public Law and Legal Theory; Legal Studies). George Washington University. https://doi.org/10.2139/ssrn.3536265

The Royal Society. (2019). *Protecting privacy in practice: The current use, development and limits of Privacy Enhancing Technologies in data analysis* [Report]. The Royal Society. https://royalsociety.org/topics-policy/projects/privacy-enhancing-technologies/

Tolmie, P. (2016, February). This has to be the cats – personal data legibility in networked sensing systems. *Proceedings of the 19th ACM Conference on Computer Supported Cooperative Work*. https://doi.org/10.1145/2818048.2819992

Urquhart, L. (2018). Realising the Right to Data Portability for the Domestic Internet of Things. *Pers Ubiqui Comput*, *22*, 317 – 332. https://doi.org/10.1007/s00779-017-1069-2

Urquhart, L. (2019). Demonstrably doing accountability in the Internet of Things. *International Journal of Law and Information Technology*, *2*(1), 1 – 27. https://doi.org/10.1093/ijlit/eay015

Wachter, S., & Mittelstadt, B. (2019). A Right to Reasonable Inferences: Re-Thinking Data Protection

Law in the Age of Big Data and AI. *Columbia Business Law Review*, *2*, 494 – 620. https://doi.org/10.7916/cblr.v2019i2.3424

Wachter, S., Mittelstadt, B., & Floridi, L. (2017). Why a right to explanation of automated decision-making does not exist in the general data protection regulation. *International Data Privacy Law*, *7*(2), 76–99. https://doi.org/10.1093/idpl/ipx005

Wagner, B. (2019). Liable, but Not in Control? Ensuring Meaningful Human Agency in Automated Decision-Making Systems. *Policy & Internet*, *11*(1), 104 – 122. https://doi.org/10.1002/poi3.198

Yeung, K. (2017). 'Hypernudge': Big Data as a mode of regulation by design. *Information, Communication & Society*, *20*(1), 118–136. https://doi.org/10.1080/1369118X.2016.1186713

Zuboff, S. (2015). Big other: Surveillance capitalism and the prospects of an information civilization. *Journal of Information Technology*, *30*, 75 – 89. https://doi.org/10.1057/jit.2015.5

Published by

Alexander von Humboldt
INSTITUTE FOR INTERNET
AND SOCIETY

in cooperation with