Evolution of Personal Data Store

Subjects: Computer Science, Cybernetics

Contributor: Khalid U. Fallatah , Mahmoud Barhamgi , Charith Perera

The idea of the personal data store goes back to the early 2000s. The initial idea of this concept was to store and capture digital materials (e.g., books, photos, and other digital documents). This idea was developed for MyLifeBits as a platform to store scanned paper files and record, store, and access a personal lifetime archive. Personal web observatories are another concept based on the idea of Personal Data Stores (PDS). A personal web observatory is a technical platform that, first and foremost, enables individuals to consolidate and archive their data that is dispersed among multiple sources. Later, the concept of Personal Information Management (PIM) and Personal dataspace management was introduced to specifically focus on the process of managing personal digital information such as emails, images, HTML, XML, audio, video, and so on.

internet of things personal data store data vaults

1. Privacy as a Driver for Personal Data Stores (PDS) to Flourish

A personal Data Store can be described as a model, framework, architecture, or ecosystem designed to give individuals ultimate control over their personal data. A person could collect, store, manage, and share his data according to his rules [1]. This definition has focused only on the fundamental processes that PDSs should have. However, other researchers further provide more details to describe PDS platforms. According to [2], a PDS is defined as “a set of capabilities built into a software platform or service that allows an individual to manage and maintain his or her digital information, artefacts and assets, longitudinally and self-sufficiently, so it may be used practically when and where it can form the individual’s benefit as perceived by the individual, and shared with others directly, without relying on external third parties”.

Furthermore, recent research initiatives have proposed better forms of PDS that empower individuals to own, control, manage, and share their personal data. The PDS model is fundamentally designed to give individuals the ability to have complete control over their data [3]. As a result, different terms have been introduced in the literature, such as Personal Data Stores (PDSs), Databox, Data Hub, Personal Information Hub, Personal Data Vaults, Personal Container, Smart Hubs, and Home Hubs.

2. Data Sovereignty as a Legal Requirement

Data sovereignty is another relevant concept to the PDS model, which is defined as the capability for individuals to have full control and determine restrictions and rules about the usage of their data (e.g., access control authorisation and usage duration) before sharing it with data consumers [4][5]. Additionally, all potential data consumers need to be transparent with the data owner. Recently, the Industrial Data Space (IDS) standard initiative proposed a reference architecture model [6]. Based on this model, data sovereignty has been considered a prerequisite for the personal data ecosystem where individuals have the ability to exploit their data as an asset for creating business opportunities for data producers and data consumers.

3. The Anticipated Advantages of PDS Model

One of the PDS model’s most prominent benefits is user empowerment. Empowering users means the ability for individuals to collect, analyse, manage, and share it with others. This also leads them to regain complete control over data processing. As a result, individuals need to give their consent for data processing and be better informed about it (e.g., potential risks, real-time logs, audits, monitoring, and visualisations). Empowerment would allow individuals to better understand how their data is being processed and feel empowered by using controlling tools provided by PDS platforms. It could also increase the trust of individuals to be more engaged in online transitions.

The second benefit would be the ability for individuals to increase the level of security by determining what, who, and when personal data can be accessed and shared [1]. Besides, regular leakages and privacy issues of even big and popular cloud-based data silos can be minimised by using the PDS model. This would be very useful to enable a decentralised platform that encourages third-party and app developers to embrace more privacy-friendly approaches [2]. Furthermore, a decentralised platform would enable new applications that combine data from many silos to draw inferences unavailable in the existing marketplace [7]. According to the literature, this model could solve and lessen many of today's issues and concerns related to privacy and data protection.

The PDS model could also be a viable solution for organisations and app developers to access a wide range of personal data (e.g., medical data, bank statements, shopping history, or fitness activities) that would be difficult, or illegal to be collected using current means. In addition to that, once the model is appropriately deployed, online service providers could easily transfer data (with data subject permission). This would then allow organisations (data consumers) to have clean, rich, and safe data. This is a dream come true for third parties, including big organisations and app developers, to perform computations and analytics with clean and rich data. Organisations could also reduce the burdens associated with acquiring and managing individuals' data.

Another promising benefit of PDS architecture is that individuals will eventually gain the capability to make profits by monetising their personal data. PDS platforms, many of which are under development, have proposed various business models to achieve this feature. For instance, some of these platforms ask data consumers (e.g., app developers) to pay per data transaction, and the type of personal data determines the price. This means an app developer could access an individual's data once consent is approved. Other platforms (e.g., PDS Mydex) require app developers to pay registration fees to be part of the PDS' ecosystem and access individuals' personal data. Alternatively, payments could also be required when app developers need to transfer and/or collective computations [8]. In return, individuals will earn small cash, discounts, or other rewards when they share their personal data.

Finally, PDS architecture is expected to provide the tools that enable individuals to analyse their personal data and gain insights about themselves. The ability to self-quantify, self-knowledge, or self-reflect has become possible due to personal informatics tools and the improved sensor technology [9]. At first, research in this area mainly focused on the utility of personal informatics. Other researchers went beyond that to suggest concentrating on the role and experience of living with data ('lived' informatics) [10][11][12]. To define personal informatics (PI), Li and Forlizzi [13] conducted surveys and interviews with people who collect and reflect on personal information. They define PI as systems that assist people in collecting relevant information intending to reflect and gain knowledge about themselves. A stage-based model was derived, in which five stages were discussed (preparation, collection, integration, reflection, and action). Some research works have developed methods that assist individuals in making sense of live data derived from smart home sensors [14][15] and reflect on their personal data and gain insights. Choe [16] built a web-based application called Visualised Self that helps users visualise and explore data. Feustel [17] examined how individuals make sense of their own data when it is presented alongside others' aggregated data. This research work investigated how people could integrate the data of others to make sense of their own data and how they identify insights and form goals without pre-existing social ties.

4. The Disadvantages of the PDS Model

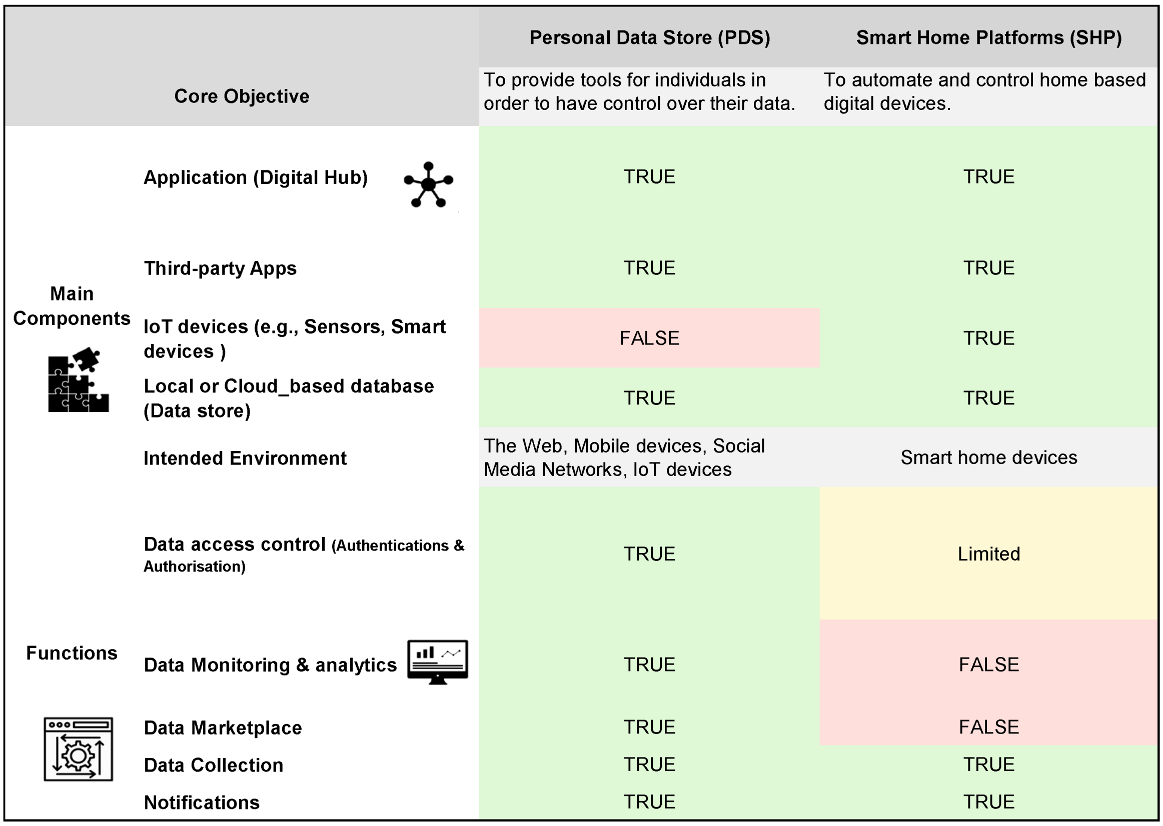
As discussed previously, the PDS model provides multiple sensible benefits for individuals regarding data protection, data sovereignty, and privacy. However, this model introduces several drawbacks that may prevent individuals from realising these benefits. The main drawback is that a potential increase of responsibility may be laid on individuals to manage and control their data, particularly for those who are not technically savvy. This also includes the burden to give and manage access and consent for data consumers, which may lead to privacy risks and unintended consequences [18]. Another important issue is data availability and accessibility, especially for local-based PDS platforms. Individuals need to securely access their personal data from anywhere and anytime. In addition, current PDS platforms are still in the early development stages and do not follow technical standards. Each platform has different security and privacy policies, terms of service, functionalities, used technologies, and systems. Thus, this may require individuals to spend a lot of time and effort before they realise the value of using PDS platforms.

5. Smart Home Platforms as a PDS

The smart home platform (SHP) is a digital home system that enables a homeowner to control, optimise, and monitor some home functions such as thermostats, lighting, air conditions, security systems, and others. These functions can be managed using software called Platforms, which act as the backbone of this digital ecosystem. A typical smart home platform is built to integrate a heterogeneous set of physical devices from various brands, such as Nest thermostats, security cameras, or smart lighting bulbs. With all these devices in place, individuals manage each device using a mobile application. This application will then allow a user to create, edit, or even delete different types of routines and automatic rules such as trigger-action routines (e.g., warn me if there is activity at my living room, turn the air condition on when I am heading home) and scheduled routines (e.g., open the curtain at my bedroom with sunrise and everyday switch all lights off at 8:00 p.m.). However, using SHP allows homeowners to have central control over multiple devices and a unified interface for accessing sensor data. Another essential feature of the smart home platform is the increase of interoperability and connectivity between smart home devices by using various proposed solutions such as a unified control platform or an open IoT platform [19][20]. As a result, users could connect smart devices from a wide range of manufacturers easily. What makes smart home platforms more fascinating is their ability to collect data related to motion, temperature, lighting control, and the state of smart devices [21][22]. This data can be handy for individuals to self-reflect and self-monitor.

Nevertheless, collecting meaningful data from smart home platforms would be challenging because they have different data storage methods [21]. In addition, smart home platforms do not provide technological solutions for individuals to store and analysis personal data. In contrast, PDS platforms are designed to collect, store, and analyse personal data from different sources. Therefore, it would be realistic and motivating to convert a smart home platform into a PDS platform. By doing so, individuals could take advantage of both platforms and can store and collect a large amount of data related to their smart home devices. Then, they would be able to use the collected data for personal analytics and data trading.

Regarding the main components and functions, SHP platforms share some similarities to PDS platforms, which can be seen in **Figure 1**. According to Kafle [23], the general architecture of smart home platforms consists of apps, devices (e.g., sensors, lighting bulbs, smart speakers, etc.), and centralised data stores where added sensors, rules, routines, and state variables of the entire smart home are stored. These components typically communicate locally over Wi-Fi networks or over the Internet. However, unlike PDS platforms, which is focused on providing the best control over personal data, smart home platforms are essentially designed to automate various aspects of physical devices ranging from small devices with little computing power to large appliances such as refrigerators.



		Personal Data Store (PDS)	Smart Home Platforms (SHP)
	Core Objective	To provide tools for individuals in order to have control over their data.	To automate and control home based digital devices.
Main Components	Application (Digital Hub)	TRUE	TRUE
	Third-party Apps	TRUE	TRUE
	IoT devices (e.g., Sensors, Smart devices)	FALSE	TRUE
	Local or Cloud_based database (Data store)	TRUE	TRUE
	Intended Environment	The Web, Mobile devices, Social Media Networks, IoT devices	Smart home devices
Functions	Data access control (Authentications & Authorisation)	TRUE	Limited
	Data Monitoring & analytics	TRUE	FALSE
	Data Marketplace	TRUE	FALSE
	Data Collection	TRUE	TRUE
	Notifications	TRUE	TRUE

Figure 1. Similarities and differences between PDS platforms and Smart Home Platforms.

6. Using PDS Platforms for Enabling Personal Data Marketplace

With the new EU General Data Protection Regulation (GDPR), individuals have become more than ever able to collect, transfer, store, and even trade their personal data. Under these new regulations, individuals have the right to transfer their data collected by firms and other service providers. However, without the use of PDS platforms, it would be difficult for individuals and data consumers to exchange data and create mutual value since there are technical challenges that both sides would face. Therefore, PDS platforms are designed and engineered to overcome these challenges by creating decentralised data marketplaces that enable all parties to share and trade personal data in several ways.

The first way is to ensure the supply of personal data by allowing individuals to gain and retrieve their data from big firms or service providers (e.g., Digi.me). This is because, currently, firms or service providers collect and own personal data. Second, PDS platforms provide tools that individuals can use to manage and control their data. This includes their ability to short, search, and transfer personal data analysis in order to transform personal data into meaningful information. Third, PDS platforms enable individuals to specify and reconfigure their security, privacy, and sharing preferences regarding data sharing and access control. Finally, PDS platforms can be seen as a potential enablers for the data-sharing marketplace because they will ultimately need to provide methods and a virtual environment where data consumers can request and negotiate access to individuals' personal data. In contrast, individuals should be able to approve requests to buy their data and receive returned value (e.g., money, discount, or free services).

7. Key Enabling Technologies for PDS Platforms

Blockchain can be viewed as a decentralised Internet infrastructure that provides a shared, immutable, and transparent history of transactions. In a blockchain network, a set of miners work together to verify and record transactions and maintain a public ledger [24]. From a technological point of view, integrating blockchains with the development of PDS platforms can provide multiple features. First, blockchains as a decentralised system can provide a robust storage system since there is no central point of failure. In addition, PDS platforms need to provide a unique identity (Self-Sovereign Identity) to associate individuals' personal data, which could lead to several other benefits, decentralised access control, decentralised data search, and decentralised data marketplace [25]. Moreover, blockchain technology helps PDS platforms with requests related to data authentications, verification, and authorisation.

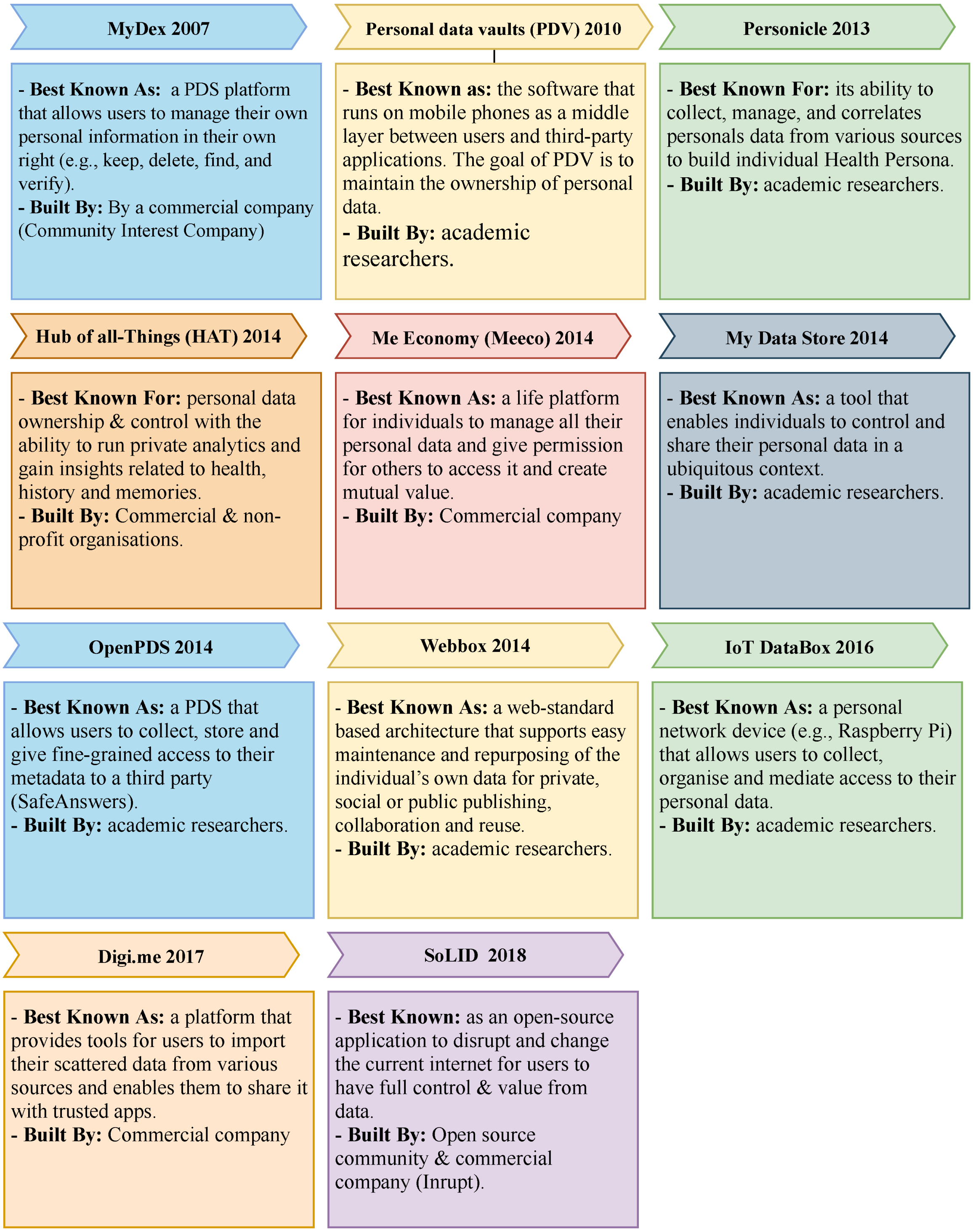
Smart contract has been introduced earlier than Blockchain, but it has been recently associated with Blockchain. This is because smart contracts are a form of self-governance and self-managed transactions that can be executed and stored automatically in the Blockchain, enabling self-governance over data. In the context of PDS platforms, smart contracts can be used as a solution for personal data determination, which refers to the ability to determine the ownership of personal data and the right to use and transfer it [24]. In SOLiD, smart contracts have been transparently defined and enforced data access policy in which individuals and service providers can deploy policies as smart contracts [26].

Semantic technologies are used to ease data interoperability, which is regarded as an essential feature of a fully functioning PDS ecosystem. This is because, in reality, PDS platforms need to effectively interact and communicate with various types of data forms, data exchange protocols, systems, heterogeneous devices, etc. Therefore, semantic technologies can facilitate interoperability through semantic annotation, managing access, resource discovery, and knowledge extraction [27]. With semantics technologies, individuals could also transfer and exchange personal data with various entities (e.g., between PDSs). For instance, RML.io (RDF Mapping Language) has been used in a proposed solution that allows individuals to transfer personal data into an interoperable format to their personal data store [28]. Furthermore, semantic technologies are used to link and organise data in decentralised stores based on authorisation methods for granting access to data. In order to automate these processes, Ref. [29], for example, used semantic web-based policy languages which allow expressing rich rules for consent and data requests.

Various other technologies have also been used to enable the existence of PDS platforms, such as Machine Learning and Artificial Intelligence (AI). In this context, the use of machine learning tools have been used to learn how to answer future third-party data requests [30], privacy preference suggestions and personalised privacy settings, and privacy preference enforcement [31]. Users of PDS can also benefit from personalised AI services by providing controlled access to their data or by asking providers to send their AI services into users' PDS [32].

8. Existing PDS Platforms

Many PDS platforms have developed over the last two decades. While some of these platforms were built by commercial companies and the open-source community, others were developed as research projects. Each of these platforms has focused on specific features to help grow and adopt the user-centric model. In the following, the researchers will discuss the development of these platforms as depicted in **Figure 2**.



MyDex 2007

- **Best Known As:** a PDS platform that allows users to manage their own personal information in their own right (e.g., keep, delete, find, and verify).
- **Built By:** By a commercial company (Community Interest Company)

Personal data vaults (PDV) 2010

- **Best Known as:** the software that runs on mobile phones as a middle layer between users and third-party applications. The goal of PDV is to maintain the ownership of personal data.
- **Built By:** academic researchers.

Personicle 2013

- **Best Known For:** its ability to collect, manage, and correlates personals data from various sources to build individual Health Persona.
- **Built By:** academic researchers.

Hub of all-Things (HAT) 2014

- **Best Known For:** personal data ownership & control with the ability to run private analytics and gain insights related to health, history and memories.
- **Built By:** Commercial & non-profit organisations.

Me Economy (Meeco) 2014

- **Best Known As:** a life platform for individuals to manage all their personal data and give permission for others to access it and create mutual value.
- **Built By:** Commercial company

My Data Store 2014

- **Best Known As:** a tool that enables individuals to control and share their personal data in a ubiquitous context.
- **Built By:** academic researchers.

OpenPDS 2014

- **Best Known As:** a PDS that allows users to collect, store and give fine-grained access to their metadata to a third party (SafeAnswers).
- **Built By:** academic researchers.

Webbox 2014

- **Best Known As:** a web-standard based architecture that supports easy maintenance and repurposing of the individual's own data for private, social or public publishing, collaboration and reuse.
- **Built By:** academic researchers.

IoT DataBox 2016

- **Best Known As:** a personal network device (e.g., Raspberry Pi) that allows users to collect, organise and mediate access to their personal data.
- **Built By:** academic researchers.

Digi.me 2017

- **Best Known As:** a platform that provides tools for users to import their scattered data from various sources and enables them to share it with trusted apps.
- **Built By:** Commercial company

SoLID 2018

- **Best Known:** as an open-source application to disrupt and change the current internet for users to have full control & value from data.
- **Built By:** Open source community & commercial company (Inrupt).

Figure 2. The evolution of the personal data store.

Hub of All Things (HAT) is a decentralised micro-server that gives individuals the full legal right to their data. This micro-server is hosted in the cloud, and personal data can be accessed using various devices [33]. Collected data from various sources can be stored and visualised. In addition, users can install tools (apps) in their micro-server to conduct private analytics and gain insights about their health, e-history, and others. With relevance to data access, users can use some technical tools to transfer their data with their permission and permit app developers to analyse their data. In return, the user can have tangible benefits such as free service. The HAT PDS can only be accessed by the owner (user) and not by HAT because users are considered here as the only controller and processors of the data within the HAT PDS.

Mydex is a PDS platform that is designed to enable users to realise the value of their data [34][35]. Users can achieve this goal by allowing app developers or data consumers to access their data. Each time they access a user's data, they have to pay a transaction fee to the PDS users, and the platform collects a percentage of each data transaction. Mydex is a cloud-based platform on which various apps can be installed. Because of encryption, only users can view data in the PDS account. However, app developers and data consumers can also view specific data once they have the required consent. In addition, the platform provides different data capture mechanisms, and users can fill in their data or let other organisations populate their PDSs.

Personal data vaults (PDV) is privacy architecture presented by Refs. [36][37][38]. PDV is software that runs on a mobile phone and communicates with PDV, which works as a middle layer between a user's mobile phone and the third-party application. PDV works like an online personal data storage, where an individual can upload personal data. It provides storage, authentication, access control mechanisms, and a user interface. The goal of this PDV is to maintain the ownership of the individual's data. PDV acts as a middle software that allows individuals to control and filter data before being shared with internet service providers. Individuals can also decide what and with whom data will be shared. However, PDV is designed for the mobile phone environment. As a result, stored data are only related to locations, movements, images, texts, and health data.

Personicle was presented as a framework that collects, manages, and correlates personal health data from heterogeneous sources and detectors events happening at a personal level [39]. Data is gained from different sensors such as Microsoft Kinect, onboard sensors on mobile phones, and wearable tracking sensors.

Meeco is similar to previous PDS in terms of empowering individuals to own and benefit directly from their data [40]. However, Meeco is more focused on helping individuals to gain insights and have the data to negotiable better outcomes.

MyData Store is a tool that enables individuals to control and share their data [41]. According to this research, MyData Store is a secured digital space owned and controlled by the user and acts as a repository for personal information. They designed this model to collect, share, and delete personal data on mobile phones. The framework provides a user-centric and data management tool that can be used through the whole lifecycle of individuals' data, from data collection and use to data trading or monetisation [42].

OpenPDS is another framework introduced by Ref. [43] intending to enable individuals to manage their data safely and privately by giving only short answers to third parties and prevent any direct access to the data. This framework is a practical way to protect the privacy of individuals. This framework proved to be viable because it was applied as a novel approach for recommender systems to overcome the limitations of the existing systems [44].

Webbox was initially introduced as a web-standard-based architecture that supports easy maintenance and re-purposing of the individual's data for private, social, or public publishing, collaboration, and reuse [45]. It was also proposed as an alternative solution to the existing online Personal Information Management (PIM) service, which does not enables users to fully control their information in terms of how it can be accessed, stored, and guaranteed (e.g., long-term persistence and security).

Databox is an alternative user-centric approach proposed to enable individuals to coordinate the collection processes and the management of their data [7]. Databox allows users to selectively and transiently share personal data with a third party for specific purposes. Later, the IoT Databox model is presented to enable internal and external accountability [46]. The IoT Databox was mainly designed as a physical device for the IoT environment. Data transfer is enabled here, and users can install apps locally. Unlike PDS HAT, Databox assigns the role of the data controller to external parties, such as app developers, when data is transferred out of the Databox, and they would not be transferred when the data is at rest in the device.

SOLiD proposed to provide a set of tools for building decentralised Web applications, including the ability for individuals to store and trade their data [47]. In addition, they offer actual data ownership, where individuals can choose where their data is stored and who can access it. Organisations can also benefit from existing data that users have already stored and use such data without needing to build up customer networks.

Digi.me provides tools for individuals to import their scattered data from apps and websites. Once data is imported, individuals would take control of the data [48]. They would also be able to search and browse that data and let third-party apps and websites integrate and access it. Digi.me claims that its business model complies with GDPR consent requirements for data processing.

KRAKEN Project is a European project that aims to develop a trusted and secure personal data platform. It enables individuals to share trade-sensitive personal data (e.g., educational and health records and well-being data from wearable devices) and their ability to maintain full control and ownership of their data throughout the entire data lifecycle [49]. The project also aims to provide individuals with advanced technological methods such as privacy-aware analytics, self-sovereign identity, and data portability control. KRAKEN, as a personal data platform solution, initially aimed to focus on the health and education sectors.

PimCity Project enables individuals to regain control of their personal data by building a platform where individuals can share and trade personal data with businesses and organisations [50]. The project delivers Personal Information Management Systems (PIMS) based on a user-centric model. The project also aims to increase transparency in the online data market by implementing a PIMS development kit (PDK) (e.g., personal data safe and personal consent management) that allows developers to engineer and experiment with new solutions.

TRUSTS Project aims to create a secure and trustworthy European market for personal and industrial data [51]. The project was initiated in 2020 by European Union's Horizon research and innovation research and is based on the experiences of two large national data-sharing projects. The platform aims to connect stakeholders, provide generic functionality, and act as a platform federation between data markets. Furthermore, the platform provides an operational and GDPR-compliant European data marketplace and follows the reference architecture designed by the International Data Spaces (IDS). The platform aims to improve the integration and adoption of future platforms by providing services to identify and overcome legal, ethical, and technical challenges across-border data markets.

References

1. Brochot, G.; Brunini, J.; Eisma, F.; Larsen, R.; Lewis, D. Study on Personal Data Stores Conducted; The Cambridge University Judge Business School: Cambridge, UK, 2015; pp. 458–459.
2. Van Kleek, M.; Smith, D.A.; Murray-Rust, D.; Guy, A.; O'Hara, K.; Dragan, L.; Shadbolt, N.R. Social personal data stores: The nuclei of decentralised social machines. In Proceedings of the 24th International Conference on World Wide Web, Florence, Italy, 18–22 May 2015; pp. 1155–1160.
3. Perentis, C.; Vescovi, M.; Leonardi, C.; Moiso, C.; Musolesi, M.; Pianesi, F.; Lepri, B. Anonymous or not? Understanding the factors affecting personal mobile data disclosure. ACM Trans. Internet Technol. 2017, 17, 1–19.
4. Duisberg, A. Legal Aspects of IDS: Data Sovereignty—What Does It Imply? In Designing Data Spaces; Springer Nature Switzerland AG: Cham, Switzerland, 2022; pp. 61–90.
5. Hummel, P.; Braun, M.; Augsberg, S.; Dabrock, P. Sovereignty and data sharing. ITU J. ICT Discov. Spec. Issue 2018, 25, 1–10.
6. Scerri, S.; Augustin, S. Industrial Data Space—Digital Sovereignty over Data. In Proceedings of the Digitising European Industry WG2 Meeting, Brussels, Belgium, 8 December 2016.

7. Chaudhry, A.; Crowcroft, J.; Howard, H.; Madhavapeddy, A.; Mortier, R.; Haddadi, H.; McAuley, D. Personal Data: Thinking Inside the Box. Aarhus Ser. Hum. Centered Comput. 2015, 1, 4.
8. Janssen, H.; Cobbe, J.; Norval, C.; Singh, J. Decentralised Data Processing: Personal Data Stores and the GDPR. SSRN Electron. J. 2020, 10, 356–384.
9. Ctrl SHIFT. The New Personal Data Landscape; Technical Report. 2011. Available online: https://www.ctrl-shift.co.uk/wp-content/uploads/2011/11/The-new-personal-data-landscape-FINAL.pdf (accessed on 23 March 2021).
10. Elsden, C.; Kirk, D.; Selby, M.; Speed, C. Beyond personal informatics: Designing for experiences with data. Conf. Hum. Factors Comput. Syst. 2015, 18, 2341–2344.
11. Ohlin, F.; Olsson, C.M. Beyond a utility view of personal informatics: A postphenomenological framework. In Proceedings of the UbiComp and ISWC 2015, Osaka, Japan, 7–11 September 2015; pp. 1087–1092.
12. Ohlin, F.; Olsson, C.M. Intelligent computing in personal informatics: Key design considerations. In Proceedings of the International Conference on Intelligent User Interfaces, Proceedings IUI, Atlanta, GA, USA, 29 March–1 April 2015; pp. 263–274.
13. Li, I.; Dey, A.; Forlizzi, J. A stage-based model of personal informatics systems. Conf. Hum. Factors Comput. Syst. 2010, 1, 557–566.
14. Kurze, A.; Bischof, A.; Totzauer, S.; Storz, M.; Eibl, M.; Brereton, M.; Berger, A. Guess The Data: Data Work To Understand How People Make Sense Of And Use Simple Sensor Data From Homes. In Proceedings of the CHI '20: Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems, Honolulu, HI, USA, 25–30 April 2020; pp. 1–12.
15. Graham, L.; Tang, A.; Neustaedter, C. Help me help you: Shared reflection for personal data. In Proceedings of the International ACM SIGGROUP Conference on Supporting Group Work, Sanibel Island, FL, USA, 13–16 November 2016; pp. 99–109.
16. Choe, E.K.; Lee, B.; Zhu, H.; Riche, N.H. Understanding self-reflection: How people reflect on personal data through visual data exploration. In Proceedings of the 11th EAI International Conference on Pervasive Computing Technologies for Healthcare, Barcelona, Spain, 23–26 May 2017; pp. 173–182.
17. Feustel, C.; Aggarwal, S.; Lee, B.; Wilcox, L. People Like Me: Designing for Reflection on Aggregate Cohort Data in Personal Informatics Systems. Proc. ACM Interact. Mob. Wearable Ubiquitous Technol. 2018, 2, 1–21.
18. Shanmugarasa, Y.; Paik, H.Y.; Kanhere, S.S.; Zhu, L. Towards Automated Data Sharing in Personal Data Stores. In Proceedings of the 2021 IEEE International Conference on Pervasive Computing and Communications Workshops and Other Affiliated Events, PerCom Workshops 2021, Kassel, Germany, 22–26 March 2021; pp. 328–331.
19. Zheng, S.; Zhang, Q.; Zheng, R.; Huang, B.Q.; Song, Y.L.; Chen, X.C. Combining a multi-agent system and communication middleware for smart home control: A universal control platform architecture. Sensors 2017, 17, 2135.
20. Javed, A.; Malhi, A.; Kinnunen, T.; Framling, K. Scalable IoT Platform for Heterogeneous Devices in Smart Environments. IEEE Access 2020, 8, 211973–211985.
21. Kim, S.; Park, M.; Lee, S.; Kim, J. Smart home forensics—Data analysis of iot devices. Electronics 2020, 9, 1215.
22. Wang, P.; Ye, F.; Chen, X. A Smart Home Gateway Platform for Data Collection and Awareness. IEEE Commun. Mag. 2018, 56, 87–93.
23. Kafle, K.; Moran, K.; Manandhar, S.; Nadkarni, A.; Poshyvanyk, D. A study of data store-based home automation. In Proceedings of the 9th ACM Conference on Data and Application Security and Privacy, Richardson, TX, USA, 25–27 March 2019; pp. 73–84.

24. Wang, H.; Yuan, Y.; Yang, F. A personal data determination method based on blockchain technology and smart contract. In Proceedings of the 2020 4th International Conference on Cryptography, Security and Privacy, Nanjing, China, 10–12 January 2020; pp. 89–94.
25. Zichichi, M.; Ferretti, S.; Rodríguez-Doncel, V. Decentralized Personal Data Marketplaces: How Participation in a DAO Can Support the Production of Citizen-Generated Data. Sensors 2022, 22, 6260.
26. Kongruangkit, S.; Xia, Y.; Xu, X.; Paik, H.Y. A case for connecting SOLiD and blockchains: Enforcement of transparent access rights in personal data stores. In Proceedings of the IEEE International Conference on Blockchain and Cryptocurrency, ICBC 2021, Sydney, Australia, 3–6 May 2021.
27. De Caldas Filho, F.L.; De Mendonça, F.L.; E Martins, L.M.; Da Costa, J.P.C.; Araújo, I.P.; De Sousa Júnior, R.T. Design and evaluation of a semantic gateway prototype for IoT networks. In Proceedings of the UCC 2017 Companion—Companion Proceedings of the 10th International Conference on Utility and Cloud Computing, Austin, TX, USA, 5–8 December 2017; pp. 195–201.
28. De Mulder, G.; De Meester, B.; Heyvaert, P.; Taelman, R.; Dimou, A.; Verborgh, R. PROV4ITDaTa: Transparent and direct transferof personal data to personal stores. Companion World Wide Web Conf. 2021, 1, 695–697.
29. Esteves, B.; Pandit, H.J.; Rodriguez-Doncel, V. ODRL Profile for Expressing Consent through Granular Access Control Policies in Solid. In Proceedings of the 2021 IEEE European Symposium on Security and Privacy Workshops, Euro S and PW 2021, Vienna, Austria, 6–10 September 2021; pp. 298–306.
30. Singh, B.C.; Carminati, B.; Ferrari, E. Learning Privacy Habits of PDS Owners. In Proceedings of the International Conference on Distributed Computing Systems, Atlanta, GA, USA, 5–8 June 2017; pp. 151–161.
31. Singh, B.C.; Carminati, B.; Ferrari, E. Privacy-Aware Personal Data Storage (P-PDS): Learning how to Protect User Privacy from External Applications. IEEE Trans. Dependable Secur. Comput. 2021, 18, 889–903.
32. Meurisch, C.; Werner, D.; Giger, F.; Bayrak, B.; Mühlhäuser, M. PDSproxy++: Proactive proxy deployment for confidential ad-hoc personalization of AI services. In Proceedings of the International Conference on Computer Communications and Networks, ICCCN, Honolulu, HI, USA, 3–6 August 2020.
33. HAT Project Research Team. HAT Briefing Paper 2: The Hub-of-All-Things (HAT) Economic Model of the Multisided Market Platform and Ecosystem; WMG Service Systems Research Group Working Paper Series (Number 02/15). 2015. Available online: http://wrap.warwick.ac.uk/65607/ (accessed on 9 November 2022).
34. Mydex CIC. The Case for Personal Information Empowerment: The rise of the personal data store. World 2010, 1–44. Available online: https://mydex.org/resources/papers/The_case_for_personal_information_empowerment/the_case_for_personal_information_en _the_rise_of_the_personal_data_store_-_a_mydex_white_paper_september_2010_final_web.pdf (accessed on 9 November 2022).
35. Papadopoulou, E.; Stobart, A.; Taylor, N.K.; Williams, M.H. Enabling data subjects to remain data owners. Proc. Smart Innov. Syst. Technol. 2015, 38, 239–248.
36. Mun, M.; Hao, S.; Mishra, N.; Shilton, K.; Burke, J.; Estrin, D.; Hansen, M.; Govindan, R. Personal data vaults: A locus of control for personal data streams. In Proceedings of the 6th International Conference on Emerging Networking Experiments and Technologies, Co-NEXT'10, Philadelphia, PA, USA, 30 November–3 December 2010.
37. Mun, M.Y.; Kim, D.H.; Shilton, K.; Estrin, D.; Hansen, M.; Govindan, R. PDVLoc: A personal data vault for controlled location data sharing. ACM Trans. Sens. Netw. 2014, 10, 1–29.
38. Shilton, K.; Burke, J.A.; Estrin, D.; Hansen, M. Designing the Personal Data Stream: Enabling Participatory Privacy in Mobile Personal Sensing. In Proceedings of the Research Conference on Communications, Information and Internet Policy, Washington, DC, USA, 16–17 September 2009; pp. 25–27.

39. Jalali, L.; Jain, R. Building health persona from personal data streams. In Proceedings of the 1st ACM International Workshop on Personal Data Meets Distributed Multimedia, Co-located with ACM Multimedia 2013, Barcelona, Spain, 22 October 2013; pp. 19–26.

40. Available online: https://www.meeco.me/ (accessed on 9 November 2022).

41. Alén-Savikko, A.; Byström, N.; Hirvonsalo, H.; Honko, H.; Kallonen, A.; Kortesniemi, Y.; Kuikkaniemi, K.; Paaso, T.; Pitkänen, O.; Poikola, A.; et al. MyData Architecture—Consent Based Approach for Personal Data Management. 2016. Available online: https://harisportal.hanken.fi/sv/publications/mydata-architecture-consent-based-approach-for-personal-data-mana (accessed on 9 November 2022).

42. Vescovi, M.; Moiso, C.; Pasolli, M.; Cordin, L.; Antonelli, F. Building an eco-system of trusted services via user control and transparency on personal data. IFIP Adv. Inf. Commun. Technol. 2015, 454, 240–250.

43. De Montjoye, Y.A.; Shmueli, E.; Wang, S.S.; Pentland, A.S. OpenPDS: Protecting the privacy of metadata through SafeAnswers. PLoS ONE 2014, 9, e98790.

44. Mazeh, I.; Shmueli, E. A personal data store approach for recommender systems: Enhancing privacy without sacrificing accuracy. Expert Syst. Appl. 2020, 139, 112858.

45. Van Kleek, M.; Smith, D.; Shadbolt, N.; Schraefel, M. A decentralized architecture for consolidating personal information ecosystems: The WebBox. In Proceedings of the Pim 2012, Seattle, WA, USA, 11 February 2012; Available online: http://eprints.soton.ac.uk/id/eprint/273200 (accessed on 9 November 2022).

46. Crabtree, A.; Lodge, T.; Colley, J.; Greenhalgh, C.; Glover, K.; Haddadi, H.; Amar, Y.; Mortier, R.; Li, Q.; Moore, J.; et al. Building accountability into the Internet of Things: The IoT Databox model. J. Reliab. Intell. Environ. 2018, 4, 39–55.

47. Mansour, E.; Sambra, A.V.; Hawke, S.; Zereba, M.; Capadisli, S.; Ghanem, A.; Aboulnaga, A.; Berners-Lee, T. A Demonstration of the Solid Platform for Social Web Applications. In Proceedings of the 25th International Conference on World Wide Web, Montreal, QC, Canada, 11–15 April 2016; pp. 223–226.

48. Available online: https://digi.me/ (accessed on 9 November 2022).

49. Gabrielli, S.; Krenn, S.; Pellegrino, D.; Spaces, J.P.B. KRAKEN: A Secure, Trusted, Regulatory-Compliant, and Privacy-Preserving Data Sharing Platform. In Data Spaces: Design, Deployment and Future Directions; Springer: Berlin/Heidelberg, Germany, 2022; pp. 107–130.

50. PIMCity—Building the Next Generation Personal Data Platforms. Available online: https://www.pimcity-h2020.eu/ (accessed on 9 November 2022).

51. FhG, L.; Heitmann, R. TRUSTS Trusted Secure Data Sharing Space D3. 9 Platform Status Report I; Technical Report 871481. 2021. Available online: https://www.trusts-data.eu/wp-content/uploads/2022/01/D3.9-Platform-Status-Report-I_Resubmission_Nov2021.pdf (accessed on 9 November 2022).

Retrieved from https://encyclopedia.pub/entry/history/show/99348