The Challenge of OwnData Service Features

A step towards an informed choice of an OwnData Service

Jan T. Frecè
E-Government Institute
Bern University of Applied Sciences
Bern, Switzerland
jan.frece@bfh.ch

***Abstract* — The goal of this paper is to raise awareness to the fact that the choice of data storage system is an increasingly significant one to make and to propose a number of dimensions to categorize such systems in a simple yet meaningful way.**

Many data subjects already use some kind of data service to store their messages, pictures, music, videos, etc. and in the light of increasing data production and a growing number of data-based services, this trend is expected to continue. Advancing from storing pop songs to storing personal health or geo-location data, however, requires data subjects to get themselves acquainted with the quality features of data storage providers, should they wish to make an informed decision.

The introduction chapter explores the consequences of the GDPR implementation in the European Union regarding the expectations towards storage of personal data, while the subsequent chapter explains the labeling decisions in this paper. The two ensuing chapters present the quality criteria for data storage widely used in contemporary reviews and completes them with additional dimensions advocated for by the author. In a final step, a quick assessment of popular data storage providers is made, using the discussed dimensions, to demonstrate the categorical imbalance in the data storage provider community.

***Index Terms*—MyData, OwnData, Personal Information Management System, Data Visualization, Personal Data Storages.**

INTRODUCTION

Data is often described as the „oil of the 21st century“. While this comparison is certainly not 100% accurate, it can be surely claimed that data is the oil of the smart city. The more data can be appraised, analyzed, and put in relation to other data points, the better the digital city model, the better the predictions and consequently the smart interventions [1]. In order to collect higher volumes and possibly a broader variety of smart city related data, all private data sources including more and more IoT devices and other sensors in private households or vehicles are rapidly gaining significance. Personal data, however, is increasingly protected by data protections laws, significantly complicating the process of legally acquiring and analyzing it. It is safe to assume that questions of data privacy will also be of growing relevance in the near future. According to the new European General Data Protection Regulation (GDPR) [2]

a) personal data belongs to the data subject.
b) irrespective of where, by whom, and on whose initiative, it has been created.
c) Personal data should not be used beyond the stated intention and has to be removed or corrected upon the data subject's notice.

During the design phase of the data architecture for the "City Platform as a Service" project [3] it became clear, that data subjects should have a broad choice of functionally different data storage providers to meet their individually differently pronounced need for privacy. Even in the case this individual need for privacy should diminish rapidly, the introduction of the GDPR fundamentally changes the flexibility of data usage and the responsibility to prove the legality of data access in connection with the intended data usage for any organization or person handling and working with foreign personal data. As keeping an own data archive of data subjects' personal data is no longer a viable option, data consumers need the data subjects to save their data somewhere shareable and accessible and trust the system to handle their privacy the way they want it to be handled.

LABELLING THE CONCEPT

The term Personal Information Management System (PIMS) as used by the European Data Protection Supervisor (EDPS) [4] will not be applied in this paper, as it already presupposes that the system is actively managing information and not merely storing data. Since both functionalities can be useful to different data subjects, neither of them shall be excluded from the definition at this point.

Another broadly used term to describe storage facilities for data subjects is Personal Data Storage (PDS). As straight forwards as it seems, this designation goes in the opposite direction than PIMS as it is omitting any sharing aspect of the process and therefore does also not cover the entire scope necessary.

Finally, the term MyData is merely describing an obvious ownership structure, leaving it to the data subject to determine, what is supposed to happen with the data. While this semantic scarcity is rather practical in this case, the term is easily confused with similarly named organizations or data concepts [5].

For all the reasons mentioned above, the term OwnData Service (ODS) shall be used in this paper to describe a service offering data subjects the chance to store their data under pre-agreed conditions. In the understanding fostered in this paper

an OwnData Service provides a data storage of some kind and offers the services minimally required by the GDPR:

1) Communication on the storage and/or processing of personal data must be provided in an easily accessible and understandable way. Systems providing the data subject with an overview of his/her data exactly serve this purpose. [2, p. 2]
2) The data subject retains the right to access, obtain and rectify his/her data at any time free of charge. [2, p. 36]
3) In addition, the data subject must be offered the possibility to move his/her data from one provider to the next without risking loss of data or having to pay additionally for such a provider change. [2, p. 36]

Optionally, an ODS provider can offer additional features like e.g. a detailed overview of structured as well as unstructured content, different methods of data sharing, the possibility to charge for data, the chance for the data subjects to gain insight by having their own data mined for them, etc. It is conceivable how for ordinary data subjects deciding upon isolated features can already be challenging. However, since such features interact, making the right choice for or against an ODS offer is even more difficult, in particular without specialized knowledge.

Although there is an infinite number of conceivable additional features and services, I argue that the six dimensions of storage, structure, sharing, portability, encryption and finally business model are the lynch pins functionally defining an ODS service. The next chapters will browse through these dimensions based on but not limited to the "main features facilitating control" listed by the EDPS for PIMS [4, p. 7] and determine why they are functionally critical for an ODS system, what their common manifestations are and which manifestations on other dimensions lead to enhanced privacy for the data subject.

CURRENT DATA SUBJECT CRITERIA

When reading data storage reviews or looking at comparison charts the criteria apparently relevant for an ODS service's quality are: price per MB, availability and compatibility of apps, and in fewer cases encryption. While such criteria have some merits, they cannot depict the entire picture. To improve the depiction, the following additional dimensions are proposed: Data storage, data structure, access mode, and payment model. The paper will also mention the categories encryption and portability but will only shortly elaborate on them since

A) assessing whether a specific encryption setup is effective and efficient requires a high number of situational information, in most cases unavailable or incomprehensible to an average data subject,
B) portability, while informative when applied to the structured minority of data, quickly loses significance when it comes to unstructured data. Due to the missing structure and/or metadata ensuring portability from one ODS provider to another, portability is reduced to the legal right of exporting the data content.

CHARACTERIZING FEATURES OF OWNDATA PROVIDERS

All ODS systems allow the data subject to exert some degree of control over its personal data. However, there are features in an ODS not merely representing an amenity to the user but rather characterizing the service's key functionality, fundamentally distinguishing it from services not exhibiting these features. The following chapters discuss six key features characterizing an ODS from a data subject's view.

Data Storage

The majority of ODS operating today is built following a centralized setup with regard to data storage[1]. Although the data itself might be physically in various locations, for this paper, if it is accessible using the same authentication, it is considered the same data location. Data stored locally by the data subject is not considered for this paper, as this is assumed to be the pre-ODS standard.

The familiar line of thought concerning centralized approaches applies for an ODS as well: There is only one provider that can fail (low risk) but if it fails all is lost (high impact). The functional importance of control over storage location(s) is clearly conceivable for inexperienced data subjects as well, as it coincides with the well-known decision, who to trust to e.g. safe-store the family-jewels or whatever might appear valuable enough to store it in a vault and chose a safe-keeper for it. The systemic question however is not who to trust, as players change on the market continuously, but what overall approach to prefer in which kind of situation.

Centralized

If the stored, centralized data has not been encrypted by the data subject prior to the upload to the ODS system, any data can be fully assessed by the ODS provider. The data in the ODS system can still be encrypted with the ODS provider holding the keys. But while this adds to the protection from outside attacks, the data subjects can merely trust, that their ODS provider will not abuse its full access to their personal data. The only way to prevent an ODS provider assessing personal data and therefore render a centralized data storage safe is by encrypting the data with keys only available to the data subject prior to the upload, thereby isolating the information from the ODS provider. By introducing this isolation, however, a direct access to the data becomes impossible and an analytical access based on encrypted computation [6] remains the only mode of data utilisation.

Decentralized

Alternatively, there is the possibility of a decentralized ODS, where the user data is stored in any number of decentralized data stores not under the control of the ODS provider, running own authorization procedures. The access conditions for data access must not be stored with nor be

[1] e.g. all solutions advertised as "in the cloud" must be considered centralized, i.e. Google Drive, IDrive, Microsoft OneDrive, iCloud Drive, the Box, Dropbox, SugarSync, etc.

accessible by the ODS provider or anybody else but the providers of the decentralized data stores themselves, as doing otherwise could reveal crucial information concerning the data subject's personal data. Therefore, in a decentralized setup, the ODS has to address the decentralized data stores when data or information concerning their data is needed and the decentralized data stores decide autonomously whether to provide the data or information or not, depending on the preferences of the data subject.

A decentralized setup hence allows for both direct access to the data as well as an analytical access, as the decentralized stores manage the data and not the ODS itself. For the same reason, unstructured as well as structured data can be handled in direct data access or in analysis access mode, with the decentralized data stores having unimpeded access to the unencrypted data, enabling them to assemble, prepare, and anonymize data extracts or analytical information without having ODS access the data directly.

Since all the data stores must operate independently the payment model for an entirely decentralized setup, combined with a high number of decentralized stores, could get complicated and laborious, though.

Data Structure

Unstructured

Unstructured ODS do not provide any additional features beyond storing the uploaded files in their systems and providing some kind of sharing mechanism. By definition they are not PIMS since they do not provide any data management functionalities, but they should nevertheless not be brushed aside. Large volumes of personal data are stored in unstructured ODS like Dropbox, Google Cloud, Microsoft One Drive & Cloud, iCloud, etc. Excluding them in this paper would mean to exclude the major part of all data stored worldwide. Therefore, and due to the improving techniques to automatically structure unstructured data [7], [8], the insight potential of unstructured data is considerable. Furthermore, unstructured ODS can provide protection against data loss, protecting the data as long as it can be transformed into structured data.

Naturally, this result could also be achieved using local, individual solutions. While such solutions can indeed provide reasonable protection against data loss and the stored files can be accessed by the data subject and/or shared with others, the skills and the resources necessary to set up and maintain such a solution cannot be assumed to be omnipresent.

Structured

Structured ODS do not only store the data subject's personal data but are also able to semantically interpret it based on its structured form. In order to excel in data interpretation, structured ODS often specialize in certain kinds of data, e.g. medical data, geo-locational data, environment sensor data, telecommunication data, etc. As these systems read and interpret the data, they are able to provide features beyond the abilities of unstructured systems when it comes to data analyses. For the data subject as well as the data consumer, a structured ODS system has advantages on an informational as well as managerial level.

On an informational level, using a structured ODS opens up the possibility of reports, visualisations, data anomaly markers, data set comparisons, and other kinds of algorithmic data interpretation for both the data consumers and the data subjects. On a managerial level, the interpreted data allows the data subject to use more complex conditions[2] managing the data access. It also allows data consumers to request data or analysis access to data more precisely, as they are able to exclude a large part of irrelevant data not by looking at the data itself but merely at the accompanying meta-data (e.g. filter commercial traffic data out of all stored traffic data before even starting an analysis). Apart from saving time and resources by lessening the computing and refining effort, this method also reduces if not eliminates 'data by-catch' not contributing to the current analysis but still containing and potentially revealing personal data. The effort of such a reduction of revealed data to the necessary minimum is characterized as "data minimisation" or "anonymisation services" by the European Data Protection Supervisor [4, p. 7].

Access Mode

When analysing data, two elements have to be combined to achieve the desired result: the analytic algorithm and the data to be analysed. Since the data subject and the data consumer each contribute one of these items, they must engage in some kind of trust-based cooperation if they want the data to be analysed.

Data Access

Traditionally the cooperation between data subject and data consumer is based on one-sided trust by the data subject towards the data consumer. The trust is one-sided, as in the majority of cases the data subject's data is sent to the data consumer to be combined with the analytic algorithm, without any possibility for the data subject to oversee what is done to its data or to ensure that only agreed operations are executed upon it.

From an effort point of view, data access is the unpretentious form of access as it can be realized in decentralized and (unencrypted) centralized setups and it allows for a multi-faceted analysis of the data.

Analysis Access

The alternative to 'data access', 'analysis access', reverses the situation and sends the analytical algorithm to the data subject, where it is executed upon the data and the analysis result is subsequently returned to the data consumer. This solution, although deemed equivalent by the European Data Protection Supervisor [4, p. 6] does, however, not solve the one-sided trust but merely reverses the trust vector. In order to rectify this, a new, trusted third party is needed: the analytics provider. As long as the analytics provider can be trusted, both parties can send the data and the algorithm to the analytics provider, who executes the algorithm upon the data and finally returns the result to the data consumer.

[2] e.g. access only allowed to data points on weekends or in case of wind speeds above 20 knots

To get rid of the pre-requirement of both parties having to trust the analytics provider, the analytics provider is only allowed to handle encrypted data using encrypted computing methods like e.g. Secure Multi Party Computation (SMPC) [9], [10] or Fully Homomorphic Encryption (FHE) [11], [12]. Consequently, the analytics provider does not have access to the data subject's data nor to the data consumer's analysis result, as both are encrypted. This design step transforms the need for a 'trusted third party' to the need of a 'third party able to perform encrypted computing'.

The shift from 'selling data' to 'granting use of data for a certain purpose under certain circumstances' can be considered significant: The data subject can be sure that its data will not be misused for an unauthorized purpose, the data consumer can be certain that the analysis will be executed exactly as instructed upon the entirety of the data volume agreed upon, and the result will be returned to the data consumer untampered. This significant shift, however, comes with a price: A third party has to be involved and compensated, the computational effort of encrypted computation is considerably higher and the degree of management necessary from the data subject's side is certainly higher, when access conditions have to be considered and defined before data is available for analysis. This increase in managerial effort from the data subject could lead to a reduced willingness to share access to data.

Payment Model

Providing an online service creates costs. The payment model determines how these costs are going to be covered. Fundamentally, there are two opposed perspectives on bearing the cost burden if no state or charity institution is willing or able to bear the costs:

Subscription

In parallel to any other service provider, an ODS provider can ask for a subscription fee to compensate for his efforts. As with providers of other services, the fee can be laid out as a flat rate, per data point managed, per data volume, per time frame, etc. As long as the subscription fee is not shaped by or depends on information the ODS provider gains from the data subjects' data (content or meta-data) in any form, the payment model is considered to be a subscription model.

Data Exploitation

Unlike e.g. a storage company with their stored furniture or a bank with the content of their vault, an ODS provider can try to cover his efforts by selling copies of the items he has been trusted to safe-store. Therefore, he can offer a payment model where the data subject does not pay any regular fee and in return permits the ODS provider to monetize the data subject's data. Naturally, it is also conceivable to use hybrid forms, such as offering the possibility to reduce the monthly subscription fee by granting permission to monetize certain data under certain conditions. Such conditions could consist of e.g. a limitation to certain categories of data (e.g. heating data, geo-location data, or a smart house's outdoor sensors), certain time spans (e.g. data older than a year), even up to a manual selection of data points. Depending on how valuable the shared data is on the market, the subscription fee is reduced. Hybrid forms are considered data exploitation even if part of the cost is covered by a regular subscription fee.

Encryption

For years, users of IT systems have been urged to encrypt their data and communications for their own protection and consequently they learned that encryption is good and protecting them. It does, however, make quite a difference, e.g.,

A) what kind of encryption is used,
B) who holds the key(s),
C) on which layer the encryption is applied.

Even with all this information revealed, a subject matter expert could not determine which combination of characteristics makes encryption solutions generally better in the context of ODS without knowing the personal goal of the data subject in question.

For example, while using a deprecated encryption cipher (example A above) is a weakness in any case, the other two example options B and C demonstrate the ambivalence of encryption:

If a data subject desires a system able to handle structured data to optimize the added value gained from it, encrypting the data without handing the key over to the ODS provider (in a centralized setup) or the decentralized data store (in a decentralized setup) would render the setup useless, as neither the ODS provider nor the decentralized data store can manage indecipherable data. On the other hand, the result coming back from an analytics provider can be encrypted in a way nobody can decipher on its own, using proxy re-encryption [13], [14]. Only the combined efforts of ODS platform and data consumer make the results readable to the data consumer. To evaluate whether encryption in these cases is a hindrance for data insight or protecting data from uncontrollable access is a matter of personal perspective and situational assessment. Consequently, the goal for the future must be an improvement of personal situational assessment when it comes to the functional properties of encryption.

Portability

Like other service providers, ODS providers do have an incentive to try implementing lock-in mechanisms for their customers in order to lower the chances of leaving customers. While this does not affect the service provided, it does affect a customer's ability to exert sovereignty over personal data and must therefore be considered as conflicting with the GDPR. To avoid miscommunication, this paper differentiates two concepts of data portability discussed in literature:

1) The DataPortability Project founded in 2008 – although using the expression 'data portability' – puts a strong focus on data interoperability. The main purpose of the project is described as promoting "the ability for people to reuse their data across interoperable applications" [15]. While data interoperability is a pre-requirement for data portability, interoperable data does not automatically lead to data portability. While the former expresses the technical compatibility of different data sets, the latter goes beyond technical pre-requirements, including legal ones,

effectively forcing the ODS provider to hand over all the data to its competition, should a data subject wish so.

2) The 'data portability' called for by the GDPR has been announced 2016 and relates to the data itself. In the GDPR guidelines 'data portability' is defined to aim at "empowering data subjects regarding their own personal data as it facilitates their ability to move, copy or transmit personal data easily from one IT environment to another" [16, p. 4]. The regulation focuses on data and therefore grants data subjects the "right to receive personal data processed by a data controller" [16, p. 4] and "transmit personal data from one data controller to another data controller" [16, p. 5]. The ODS provider must include all "personal data concerning the data subject" [16, p. 7] as well as "data provided by the data subject" [16, p. 8]. This idea of data portability strives for an environment where data subjects can choose among a selection of ODS providers with different services and conditions and move their personal data between them freely never having to fear being locked in.

For this paper, only the GDPR definition of data portability will be used, since the older definition by the DataPortability Project merely addresses the question of data format (explicitly) and access to data (implicitly), but neglects to bring up the crucial points of having the opportunity to move data and/or the access to data from one ODS provider to another without having to fear a lock-in situation. In contrast to the other dimensions discussed in this paper, the dimension of portability is not conceived to express more than one acceptable characteristic against the background of GDPR's regulations. Its mentioning as last dimension is rather aimed at ensuring a GDPR-based understanding of the term 'data portability' when characterizing ODS providers.

Quick Assessment of popular ODS Providers

With growing volumes of personal data and the increasing need to organize and manage them, the question will not be whether the majority of data subject uses an ODS but how the data subject is supposed to choose the best ODS for its needs. For an inexperienced data subject, it is almost impossible to perform a founded appraisal of ODS providers in order to have his/her needs met. To facilitate orientation in this market, the dimensions discussed above are suggested for an overview appraisal. As a demonstration of the suggested approach and to provide a glimpse on the current ODS market, selected ODS providers are analysed using the six dimensions discussed above. The ODS providers have been selected either based on their widespread use (Google Cloud [17], iCloud [18], Dropbox [19], Microsoft Drive [20] & Cloud [21]) or based on their profile as a specialised ODS provider (MyData [5], MiData [22]).

Data Storage & Access Mode

The storage dimension reveals a considerable imbalance in favour of centralized solutions. With only one exception, all ODS providers considered relying on storing all personal data centrally in their own sphere of influence. The only exception in this regard is the Nordic MyData concept which strives "to convert data from closed silos into an important reusable resource" [5, p. 2].

With centralized storage, full data access is an inevitable consequence, unless the data subject exclusively holds the encryption keys. None of the considered ODS providers, however, mentions an encryption layer for the data subject. The combination of these two factors result in a situation where all personal data is concentrated in one location managed by the ODS provider and protected by an encryption accessible to the same ODS provider. Consequently, the data subjects have no other choice than to trust their ODS providers, since they do not have the means to detect, let alone prevent an unauthorized handling of personal data.

The MyData approach, allowing for decentralized data stores, is the only considered ODS provider that could offer analysis access to its users, providing the decentralised data stores have the necessary functionality at their disposal. There are, for the time being, however, no indications that such a functionality is currently in place nor planned.

Data Structure

Regarding the question whether data can be handled in a structured and/or instructed way, there is a range of options. While the two specialised ODS providers (MyData and MiData) are able to handle structured data of pre-defined categories, unstructured data is not mentioned as in-scope. The major-league ODS providers all offer storage for unstructured data and, with the exception of Dropbox, they all also offer to store structured data of pre-defined categories.

Payment Model

With one exception, all considered ODS providers operate with a subscription model, most including a small amount of storage space for free. The MyData concept allows for a greater flexibility giving ODS providers the freedom to implement alternative payment models, however no documentation of such a implementation could be discovered.

MiData on the other hand, operates on a non-monetary basis resting upon the voluntariness of the data subject. Consequently, the data subjects are not compensated for their data donation but the income generated from it is directed towards improving the platform and the services of the non-profit organisation.

Portability

Portability of structured data has to rely on the same ontology being used or translation tables being available. With sites like schema.org, founded already in 2011 to collect, arrange, and host ontologies for hundreds of data types, the groundwork for data portability has been laid. Unfortunately, the dissemination of these standards has not yet reached a level where they could be described as dominant. Nevertheless, the trend is emerging in the right direction, with numbers increasing year by year [23].

Conclusion and future research

While the sample size is too small to allow for universally valid statements, it nevertheless facilitates to determine current trends and needs for future research.

Centralized storages dominate the market and since the GDPR is not a globally valid regulation, this trend is not expected to change radically. But with the upcoming of platforms dedicated to a decentralized access and structured data the path towards more sophisticated services using techniques like analysis access seems to be open. Whether data subjects will be willing to accept more complex platforms demanding a higher management effort from their side remains to be seen.

Future research regarding the features of ODS should be concentrated on three main topics: easier understanding and better visualization of encryption, ability to convert between ontologies, and a better inter-linkage of data storages, as progress in these topics would forward the autonomy of the data subjects, their flexibility and independence.

ACKNOWLEDGMENT

The CPaaS.io project [3] has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 723076 as well as Japan's National Institute of Information and Communications Technology under management number 18302.

REFERENCES

[1] M. Batty, "Big data, smart cities and city planning," Dialogues Hum. Geogr., vol. 3, no. 3, pp. 274–279, 2013.

[2] European Parliament, General Data Protection Regulation. Brussels, 2016.

[3] S. Haller, "City Platform as a Service – Integrated and Open," 2016. [Online]. Available: https://cpaas.bfh.ch/. [Accessed: 30-Apr-2017].

[4] European Data Protection Supervisor, "EDPS Opinion on Personal Information Management Systems," Brussels, 2016.

[5] K. Kuikkaniemi, A. Poikola, and H. Honko, "MyData – A Nordic Model for human-centered personal data management and processing," Ministry of Transport and Communications, Helsinki, 2015.

[6] S. Goldwasser, Y. T. Kalai, R. A. Popa, V. Vaikuntanathan, and N. Zeldovich, "How to Run Turing Machines on Encrypted Data," Lect. notes Comput. Sci., no. 8043, pp. 536–554, 2013.

[7] T. K. Das and P. M. Kumar, "BIG Data Analytics: A Framework for Unstructured Data Analysis," Int. J. Eng. Sci. Technol., vol. 5, no. 1, pp. 153–156, 2013.

[8] J. Gardner and L. Xiong, "An integrated framework for de-identifying unstructured medical data," Data Knowl. Eng., vol. 68, no. 12, pp. 1441–1451, 2009.

[9] G. Zyskind, O. Nathan, and A. Pentland, "Enigma: Decentralized Computation Platform with Guaranteed Privacy," Cambridge, Mass., Jun. 2015.

[10] U. Maurer, "Secure multi-party computation made simple," Discret. Appl. Math., vol. 154, no. 2, pp. 370–381, 2006.

[11] C. Gentry, "Implementing Gentry's Fully-Homomorphic Encryption Scheme Preliminary Report," Organization, pp. 1–30, 2010.

[12] M. Clear and C. McGoldrick, "Multi-identity and multi-key leveled FHE from learning with errors," Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics), vol. 9216, pp. 630–656, 2015.

[13] G. Ateniese, K. Benson, and S. Hohenberger, "Key-Private Proxy Re-encryption," Top. Cryptol. - Ct-Rsa 2009, Proc., vol. 5473, pp. 279–294, 2009.

[14] P. Wei, X. A. Wang, and X. Yang, "Proxy re-encryption schemes with proxy having its own public/private keys," in 2010 2nd International Workshop on Database Technology and Applications, DBTA2010 - Proceedings, 2010.

[15] Faraday Media, "DataPortability Project." [Online]. Available: http://dataportability.org/. [Accessed: 02-Feb-2017].

[16] European Commission, Guidelines on the right to data portability. 2016, p. 15.

[17] Google Inc., "Google Cloud Computing, Hosting Services & APIs | Google Cloud Platform." [Online]. Available: https://cloud.google.com/. [Accessed: 29-Apr-2017].

[18] Apple Inc., "iCloud." [Online]. Available: https://www.icloud.com/. [Accessed: 29-Apr-2017].

[19] Dropbox Inc., "Dropbox." [Online]. Available: https://www.dropbox.com/?landing=cntl. [Accessed: 29-Apr-2017].

[20] Microsoft Inc., "Microsoft OneDrive." [Online]. Available: https://onedrive.live.com/about/en-us/. [Accessed: 29-Apr-2017].

[21] Microsoft Inc., "Microsoft Cloud." [Online]. Available: https://cloud.microsoft.com/en-us/. [Accessed: 29-Apr-2017].

[22] MiData Cooperation, "MiData." [Online]. Available: https://www.midata.coop.

[23] R. V Guha, D. Brickley, and S. MacBeth, "Schema.org: Evolution of Structured Data on the Web," Queue, vol. 13, no. 9, pp. 10–37, 2015.

[24] M. Brenner, "Computational Health Informatics - WAHC'17," 2017. [Online]. Available: https://www.chi.uni-hannover.de/wahc17. [Accessed: 29-Apr-2017].

[25] H. Tang et al., "Protecting genomic data analytics in the cloud: state of the art and opportunities.," BMC Med. Genomics, vol. 9, no. 1, p. 63, Oct. 2016.