MPhil Technology Policy

2014-2015

FINAL GROUP PROJECT

PERSONAL DATA STORES

CLIENT

EUROPEAN COMMISSION

STUDENTS

GUILLAUME BROCHOT, JULIANNA BRUNINI, FRANCO EISMA

REBEKAH LARSEN, DANIEL J. LEWIS

ACADEMIC SUPERVISOR

DR. JIN ZHANG

We confirm that this piece of work is our own unaided effort, except as specified herein, and that it conforms to the Cambridge Judge Business School's guidelines on plagiarism; all sources are fully acknowledged and referenced. The submission does not contain material that has already been used to any substantial extent for a comparable purpose.

PROJECT AVAILABILITY:

Available (To Cambridge University staff and students only)	
Consult (Prospective readers will be directed to email for permission to read your project) Contact email address is:	
Confidential until this date:	

Would you like a copy of your project to be made available online via the Cambridge Judge Business School website? Email *weboffice@jbs.cam.ac.uk* for more information.

UNIVERSITY OF CAMBRIDGE
Judge Business School

Self-Published

The consultancy advice of the Project Team is offered to the client in good faith and free of charge (beyond expenses). No liability for any errors, omissions or consequential problems can be assumed by the University or its students. Clients are advised to conduct their own independent assessments before implementing any suggestions made by the Project Team.

First printing, May 2015

Contents

List of Figures

List of Tables

Acknowledgements

This report is the result of a capstone consulting project conducted at the Judge Business School, University of Cambridge. As the students involved in this project, we would like to express our gratitude to the following organisations and individuals for providing resources, background, guidance, and encouragement.

First, we would like to thank the European Commission (EC) for this opportunity, and more specifically, those involved in various departments of the Directorate General for Communications Networks, Content, and Technology. The team in Unit H.4 (Trust and Security) provided a wealth of resources, a much-needed legal background, and a week of informative interviews with Commission representatives in Brussels. We would like to thank in particular Mr. Robert Madelin for his encouragement in this partnership between the EC and the Judge Business School, Mr. Malte Beyer Katzenberger and Ms. Céline Deswarte for providing resources and insight, and Mr. Raffaele Di Giovanni Bezzi for his excellent guidance, his time setting up various interviews, and his feedback throughout the entirety of the project.

We would also like to thank the following industry representatives, who generously donated their time and insights through a series of interviews and follow-up communications:

- Cozy Cloud
- Digi.me
- Midata.coop
- Mydex
- Patients Know Best
- Pryv
- Synergetics
- The Respect Network
- Qiy

Finally, we would like to thank those at the University of Cambridge who also contributed to this project:

- Dr. David Erdos (Department of Law) for his insights into data protection regulation and application to personal data spaces.
- Those researchers at the Computer Lab who provided resources and insight into technical as well as social aspects of the PDS concept.
- Dr. Jin Zhang (Judge Business School), for her excellent guidance and economic insight.

Executive Summary

The European Commission's Directorate General for Communications Networks, Content & Technology (DG CNECT) commissioned this report to evaluate whether the Personal Data Store (PDS) concept is a viable mechanism to increase consumer trust and engagement in the Digital Single Market. The report explores the PDS concept from social, legal, technical, and economic perspectives, recommending ways to guide development of the innovation. The report also explores PDSs specifically in the healthcare sector to provide a concrete case study.

Personal data stores enable individuals to regain control of their personal data. This user-centric model could offer individuals more convenience, new forms of remuneration and data management tools, in addition to a new means to exercise their digital rights. It could provide new opportunities for innovative growth, enable new and more comprehensive research, open up big data analytics to smaller firms, and provide efficiency gains to public sector organisations in particular.

Advances that blend law and technology may alleviate some of the legal challenges PDS providers currently face. For instance, protocols called 'sticky policies' wrap the data in an envelope of consent and control agreements. The data thus travels with its consent and control expectations, ensuring that only those third-parties that meet the usage agreements can access the underlying data. The main challenge to widespread adoption is interoperability, which is limited by coordination issues and misaligned incentives.

Summing expected economic benefits to organisations and to consumers, the value-creation potential of personal data applications is estimated at close to €1 trillion annually by 2020. Personal data stores may play an important role in unlocking the value of personal data applications. The potential market size for PDS providers in the EU is estimated to be some €1 billion to €91.9 billion.

As an innovative concept, the personal data store faces significant obstacles to widespread diffusion. In particular, PDS providers must reach critical mass in the context of a double-sided market: the PDS system must attract a sufficient number of individuals and businesses if it is to flourish as a platform for data exchange, but neither individuals nor businesses are easily captured without the other first in place. Current PDS providers have attempted a range of strategies to address this dilemma, from targeting a user group to fill both sides to proposing traditional services and eventually adding more specialised capabilities.

Given the social, legal, technical, and economic challenges facing the PDS ecosystem, the European Commission might:

- Educate consumers about data management and the PDS concept;
- Commission research to further explore consumers' behaviour regarding privacy, control, and convenience;
- Harmonise regulatory regimes and provide more education and consultation opportunities for SMEs to navigate compliance requirements;
- Facilitate platform interoperability through the discussion and promotion of industry standards, coordination, and networking;
- Consider helping PDS providers reach a broader user-base, perhaps through public procurement programs or dialogues with telecoms;
- Connect PDS providers to other personal data stakeholders through conferences and networking events to foster the exchange of ideas, connections, and interoperability;
- Make funding sources widely visible and simple to understand.

Part 1

1. Background & Motivations

Over the past two decades, a combination of elements has created a data-rich world: cost reductions in data storage, data analysis and cloud computing; the rapid spread of personal computing, mobile devices and social networking; and improvements in internet connectivity and speed. In this world, personal data represents value; the European Consumer Commission has deemed data 'the new oil'[1], the World Economic Forum has deemed it 'a new asset class'[2], and the academic community agrees that 'a data gold rush' is upon us[3].

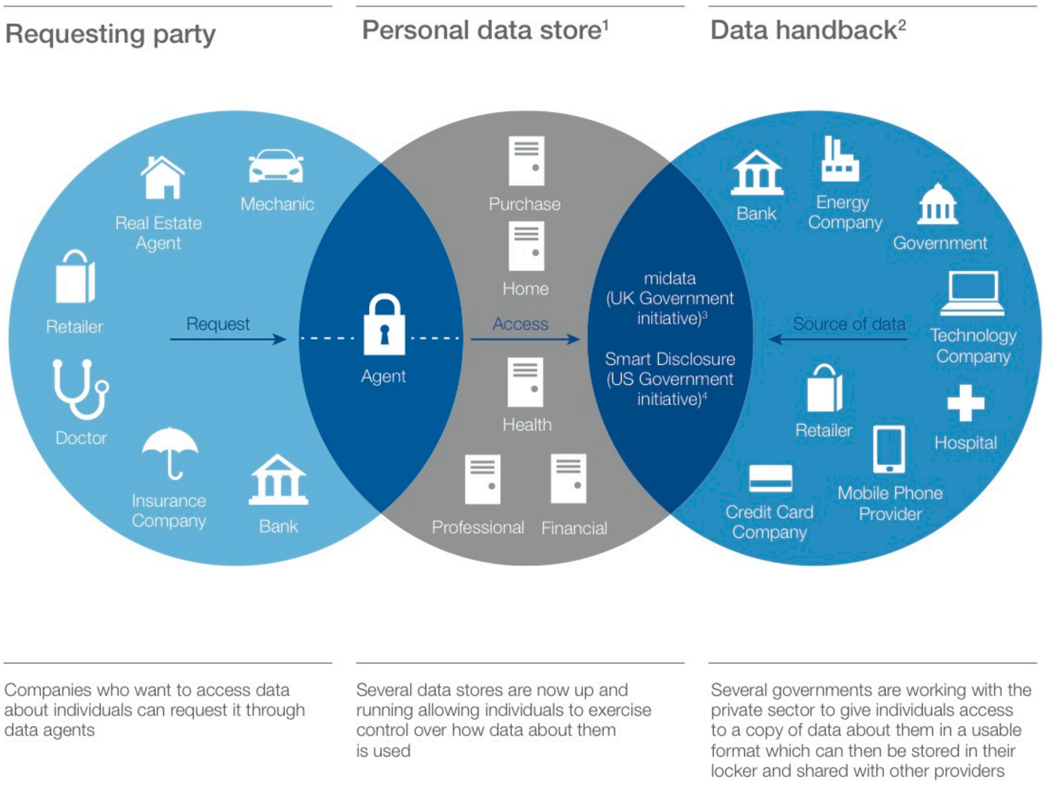
Though the 'data rush' offers significant economic and social value, it depends on trust. In light of geopolitical events such as the Snowden revelations, the increasing frequency and magnitude of data breaches, and increased discussion about necessary rights in the digital age, the public has become increasingly concerned with personal data control[4,5].

Because trust is crucial to a properly functioning market[6], the public's mounting skepticism is concerning. The digital single market is an EU priority which aims to eliminate barriers to cross-border flows of goods, services, capital and labour within the EU for digital goods and services[7]. The European Commission has estimated that EU consumers could save €11.7 billion each year if the entire range of online goods and services across the single market were available to each consumer[8]. Increased participation of both organisations and individuals in the digital single market would create substantial growth; according to McKinsey's Global Institute, the internet economy has accounted for ∼21% of GDP growth in the last five years in the G8 countries and is also responsible for significant employment[9]. In France for example, the internet economy has been responsible for ∼25% of net employment creation. A failure to complete full integration of the digital single market would entail expected lost gains of ∼4.1% of GDP by 2020[10].

Necessity is the mother of invention, and in light of growing concerns an opportunity is emerging. New personal data technologies seek to empower individuals to collect, store, manage, use, and share their personal data according to their own levels of privacy comfort, trust, and needs. This report aims to contribute to the European Commission's consultation process on 'user-controlled, cloud-based technologies for storage and use of personal data'[11]. Whether called personal data 'vaults', personal data 'lockers', 'personal clouds', or, as this report chooses, 'personal data stores' (PDSs), all such technologies share the following features:

> **Personal Data Store:** A personal data store is a technology that enables individuals to gather, store, update, correct, analyse, and/or share personal data. Of particular importance is the ability to grant and withdraw consent to third parties for access to data about oneself (See Figure 1[12] on Page 3).

[1] Kuneva, *Keynote Speech*, 2009, Roundtable on Online Data Collection, Targeting and Profiling, Brussels.
[2] Forum and Group, *Rethinking Personal Data: Strengthening Trust*, 2012.
[3] Haddadi et al., "Personal Data", 2015.
[4] Cavoukian and Reed, "Big Privacy", 2013.
[5] Davos, "The Snowden effect", 2014.
[6] Akerlof, "The Market for "Lemons": Quality Uncertainty and the Market Mechanism", 1970, pp. 488–500.
[7] Martens, "What does economic research tell us about cross-border e-commerce in the EU Digital Single Market?", 2013.
[8] European Commission, *A Digital Single Market Strategy for Europe.* 2015.
[9] Manyika et al., *Open Data: Unlocking Innovation and Performance with Liquid Information*, 2013.
[10] Alexandru, Irina, and Alice, "Consumers Attitude towards Consumer Protection in the DSM", 2014.
[11] European Commission, *Towards a thriving data-driven economy*, 2014, Brussels. COM(2014) 442 final, p. 11.
[12] World Economic Forum and The Boston Consulting Group, *Unlocking the Value of Personal Data: From Collection to Usage*, 2013.



Companies who want to access data about individuals can request it through data agents

Several data stores are now up and running allowing individuals to exercise control over how data about them is used

Several governments are working with the private sector to give individuals access to a copy of data about them in a usable format which can then be stored in their locker and shared with other providers

Figure 1: Personal data stores offer individuals numerous benefits, including control, organisation, easy-updating, sharing and analytical capabilities; some PDSs may focus on a single theme (e.g. health data), while others may offer a single point of access to any number of data collections. Importantly, individuals can specify sharing preferences to grant and rescind third-party access to their data.

The personal data store (or personal data space) is a concept, framework, and architectural implementation that shifts data acquisition and control from a distributed data model to a user-centric model (See Figure 2 on Page 4, adapted from Patients Know Best[13]). It is a technologically-enabled means to regain control of data access - with the ability to grant and withdraw consent for their data to be processed.

The PDS concept could also provide significant individual and economic benefits by enabling more targeted, personalised services to users through the integration of third-party providers into a PDS ecosystem. Such third-party services could make use of cleaner, more accurate, user-curated services to provide for a customised level of service unique to each customer's needs and desire to share, adding significant value.

This model may allow individuals to gather, store, update, correct, analyse, and share their personal data with full fundamental control. This is also a marked deviation from the existing environment where distributed data is stored throughout organisations and companies internally, with limited-to-no access or control from the user whom the information is about. As it will be demonstrated below, a user-centric personal data store model would not only rebalance the level of data control between companies and individuals but would also enable significant positive externalities for society including economic growth, increased consumer trust, increased engagement in the digital single market, research benefits through big data analytics, health-care efficiency and effectiveness improvements, and other public sector cost-savings and benefits.

[13] Patients Know Best, *Welcome to the world's first patient-controlled medical record*, 2015.

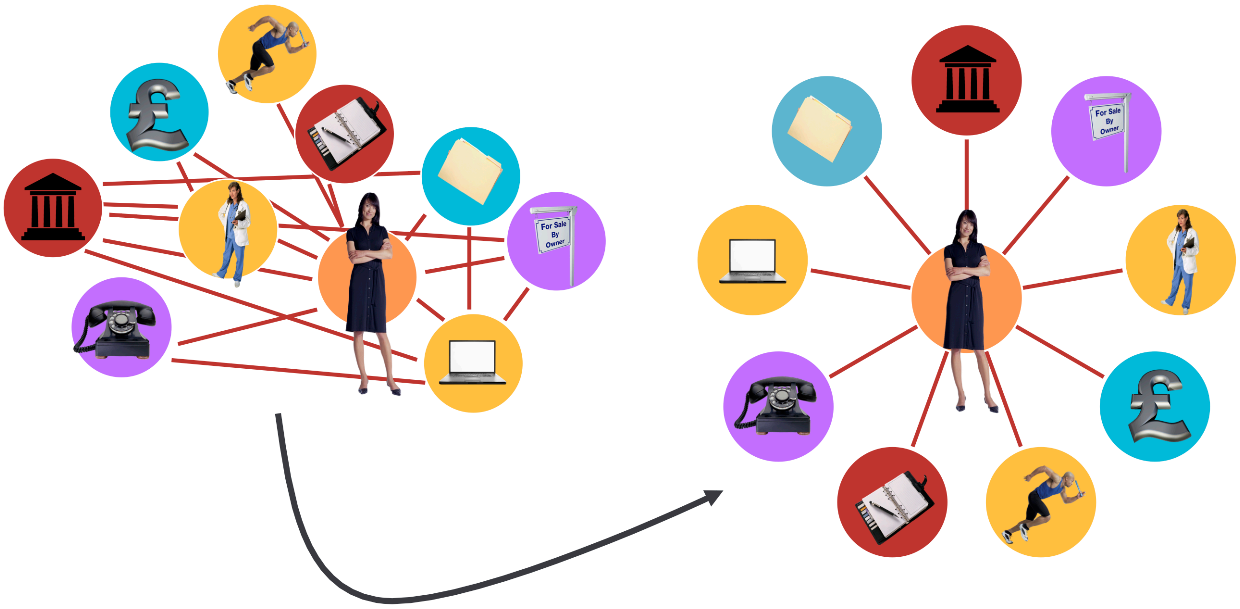


Figure 2: Personal data stores would shift data storage from its current, distributed model–in which data is partitioned into silos controlled by third parties–to an individual-centric model. Figure adapted from Patients Know Best (2015)

The PDS is one example of an innovation that could facilitate a fundamental shift in the way data is managed online. The current data ecosystem is a complex mix of emerging firms and large established incumbents across a diverse range of sectors, including:

1. Multinational corporations, some of which derive revenue from data monetisation, and others with more diverse revenue streams[14,15,16,17] (e.g. Google vs. Apple);
2. Small and medium enterprises ('SMEs');
3. Highly-regulated telecommunications companies, private healthcare providers, financial institutions;
4. Public sector regulatory bodies;
5. Public sector organisations such as hospitals, schools, police departments and passport issuing agencies.

Currently, these players collect personal data and control it internally, resulting in a siloed data ecosystem[18]. As a result, individuals can only access and manage the information stored about them with the relevant organisation's assistance, and generally under the parameters established by each organisation.

Shifting data management to personal data stores would devolve control from companies and organisations to individuals. The multinationals, SMEs, regulated industries, public sector regulators, and public sector agencies mentioned above would still be significant players in the new PDS ecosystem. However, a new middleman would stand between these data-interested players and the data subjects themselves: PDS providers.

As the radial chart shows (See Figure 3[19] on Page 6), independent PDS providers may be well equipped to maximise the benefits of data analytics while preserving the protection of individual rights. The figure ranks five characteristics of PDS ecosystem players from 'low' to 'high': the incentive to offer consent-based control to users; the incentive to protect – rather than sell or disseminate – user's personal data; the diversity of the data collected by the player; the big data potential that the player's datasets hold; and the number of

[14] BUSINESSMODELINNOVATIONMATTERS, *Comparing Facebook and Google Business Models*, 2012.

[15] Pijl, *Facebooks' Business Model Visualized - Business Model Innovation Hub*, 2011.

[16] Parr, *The Google Revenue Equation, and Why Google's Building Chrome OS*, 2011.

[17] Taylor, *Apple's Business Model Is Backwards — And It Works Like Crazy*, 2013.

[18] Cavoukian and Green, *Privacy by Design and the Emerging Personal Data Ecosystem*, 2012.

[19] Lewis, *Radar Charts Illustrating PDS Ecosystem*, 2015.

users in the player's network. The radial axes are defined such that plot area offers a visual cue: the larger the coloured area, the greater the potential non-commercial benefits.

This report discusses how a user-centric model might rebalance the distribution of power between companies and individuals, increase consumer trust, bring about new research opportunities through big data analytics, and facilitate public sector cost-savings. Chapter 2 (Page 9) highlights such social benefits and their associated concerns as well as legal considerations. Chapter 3 (Page 20) describe some of the technical concerns and potential technologies facilitating PDSs. A user-centric, privacy-friendly ecosystem may also enhance EU citizens' engagement in the digital single market and overall economic growth. These implications appear in Chapter 4 (Page 28), which also explores the challenges PDS providers face when presenting their business models to the market. The conclusion (See Chapter 5 on Page 54) recommends ways in which the European Commission might facilitate the development of a European PDS ecosystem.

Health Case Study

Because the 'personal data store' concept is new and, as a result, high-level, the report supplements each section with a case study grounded in specific examples. Each case study relates to mHealth for the following reasons:

First, individuals consider health data to be some of the most sensitive information related to their person. As the Twitter histogram shows (See Figure 4 on Page 7), health-related terms account for 5 out of the 10 most frequent tags chosen for tweets related to personal data privacy. Studies that measure Europeans' willingness to exchange data for money point to the same conclusion (See Figure 5 on Page 7): 50% of European survey respondents would agree to exchange their age and gender data for less than €1, but not even 50% would agree to exchange their health record for €50[20].

Secondly, the social benefits of mHealth PDSs are clear. Putting patients in control of their health data offers them:

- Faster, more efficient access to care;
- A better understanding of their own health;
- Access to remote care;
- Greater mobility between healthcare providers, throughout the world;
- Integration with mobile devices, fitness, and health apps.

In addition, putting patients in control of their health data also has the potential to offer society:

- Altruism, and an impact on broader social benefits;
- Significant reductions in public healthcare expenditures;
- The benefits of big data analytics in medical research, which is especially valuable for rare diseases.

The economic benefits of mHealth PDSs are also clear. Healthcare providers save money by spending less time gathering information about patients, and fewer emergency room admittances and test duplications are necessary. Big data could enable more efficient public and private medical insurance and prevent fraud[21]. According to The Boston Consulting Group[22], the public sector and health care industry stand to profit most from personal data applications and are expected to realise 40% of the total organisational benefit.

Finally, the healthcare sector operates in a complex regulatory and legal environment. There are stringent legal requirements related to the processing of health data, as it is sensitive data, and there is heterogeneity in the regulatory environment because healthcare is predominantly a Member State competence in the EU. If healthcare PDS providers can be successful, it bodes well for PDS providers in similarly complex industries, like finance and insurance. ■

[20] Boston Consulting Group, *The Value of Our Digital Identity*, 2012.

[21] Manyika et al., *Open Data: Unlocking Innovation and Performance with Liquid Information*, 2013.

[22] Boston Consulting Group, *The Value of Our Digital Identity*, 2012.

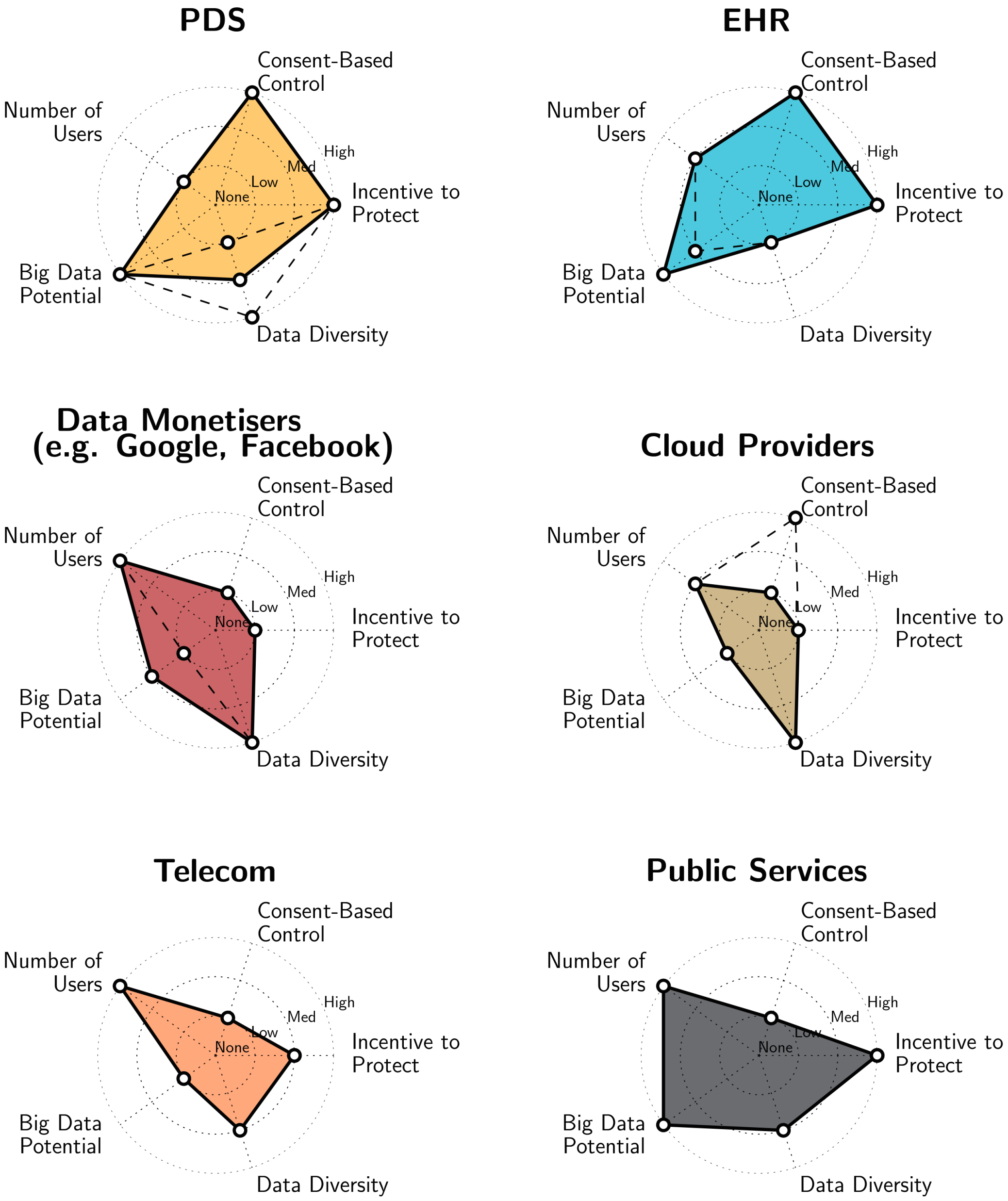


Figure 3: Comparison of today's data ecosystem players along five metrics; 'number of users' refers to the size of the player's network; 'consent-based control' refers to the individual user's ability to edit, extend and rescind access to the information being stored about them; 'incentive to protect' refers to the alignment of the data player's interests and the individual user's interests in terms of protecting the individual's data; 'data diversity' refers to whether the data the player collects data of one type (e.g. health data) or of many types; 'big data potential' refers to the combination of large data sets and clear consent mechanisms for alternative uses with social impact, such as health research.

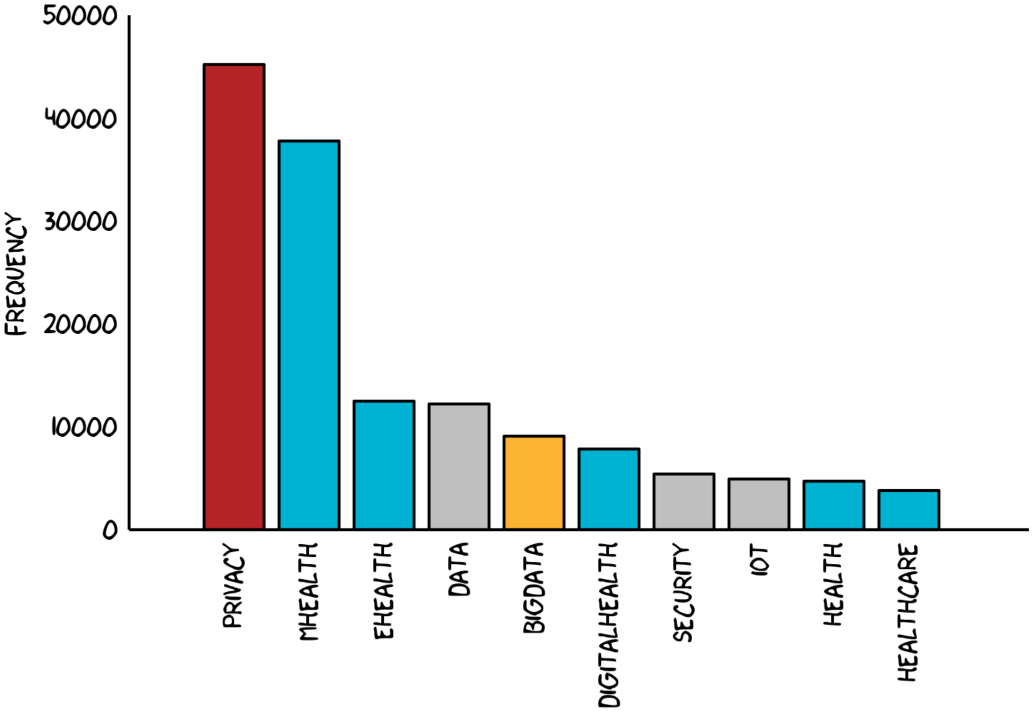
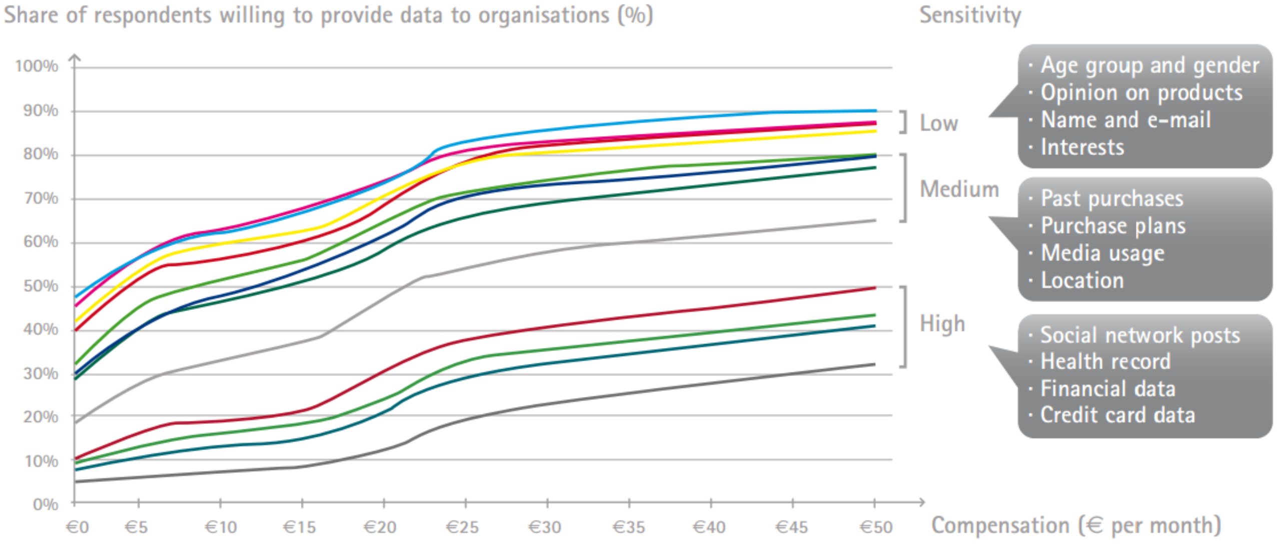


Figure 4: Frequency of tags chosen for tweets related to personal data; total number of tweets in the sample was 350,000.



Source: BCG digital identity survey (n = 3,107, August 2012)

Figure 5: Monetary compensation demanded by survey respondents to share various categories of sensitive data with organisations; (n = 3,107)

II

Part 2

2. Social & Legal Considerations

2.1 Introduction

The current paradigm surrounding the collection, storage, use, and monetisation of personal data leaves lingering social concerns from both the individual and organisational perspectives. There exists a severe data control imbalance between organisations and individuals with most users seeing personal data and its organisation-centric management as a threat and a risk, a hassle and a chore, and a source of frustration and irritation, with breaches of privacy ranging from minor to severe[23]. From the perspective of organisations, it is increasingly understood that the collection of larger quantities of personal data is expensive, corrosive of client trust, and difficult to utilise.

This current state of affairs is not ideal for either side when it comes to the exercising or protection of data processing rights. For individuals, it is not entirely clear how their personal information is or could be managed, having potentially detrimental effects on rights to data access, erasure, portability, privacy, etc. For organisations (particularly in the EU, where there exist disparities between data protection laws in each member state), the compliance overhead within multiple regulatory regimes represents a substantial liability risk and operational burden.

The PDS system, if based on informed and explicit consent and developed with the appropriate protections, infrastructure, and services, aims to empower data subjects by devolving personal data back into their control[24]. It offers individuals new convenience, remuneration and data management tools, as well as tools for and clarity in exercising a plethora of their digital rights. Thus, it could also benefit society as a whole by: facilitating engagement in the DSM, providing new opportunities for innovative growth, enabling new and more comprehensive research, opening up big data analytics to smaller firms, promoting a more rights-respecting digital environment, and providing efficiency gains particularly in the healthcare and public sector.

Although a PDS ecosystem offers individuals and society numerous benefits, it also requires that the ecosystem builders fully consider the trust and security concerns it elicits. Even if data is not centralised in its physical storage, the apparent centralisation via a single interface will almost certainly lead to a plethora of trust and control concerns. This is greatly because of diversity: of users, their attitudes, their needs, and of the many contexts of data processing[25].

With this inherent complexity in mind, below is an examination of social and legal considerations relevant to the PDS system – both benefits and concerns.

2.2 Social Considerations for a PDS System

2.2.1 Potential PDS Benefits for Individuals

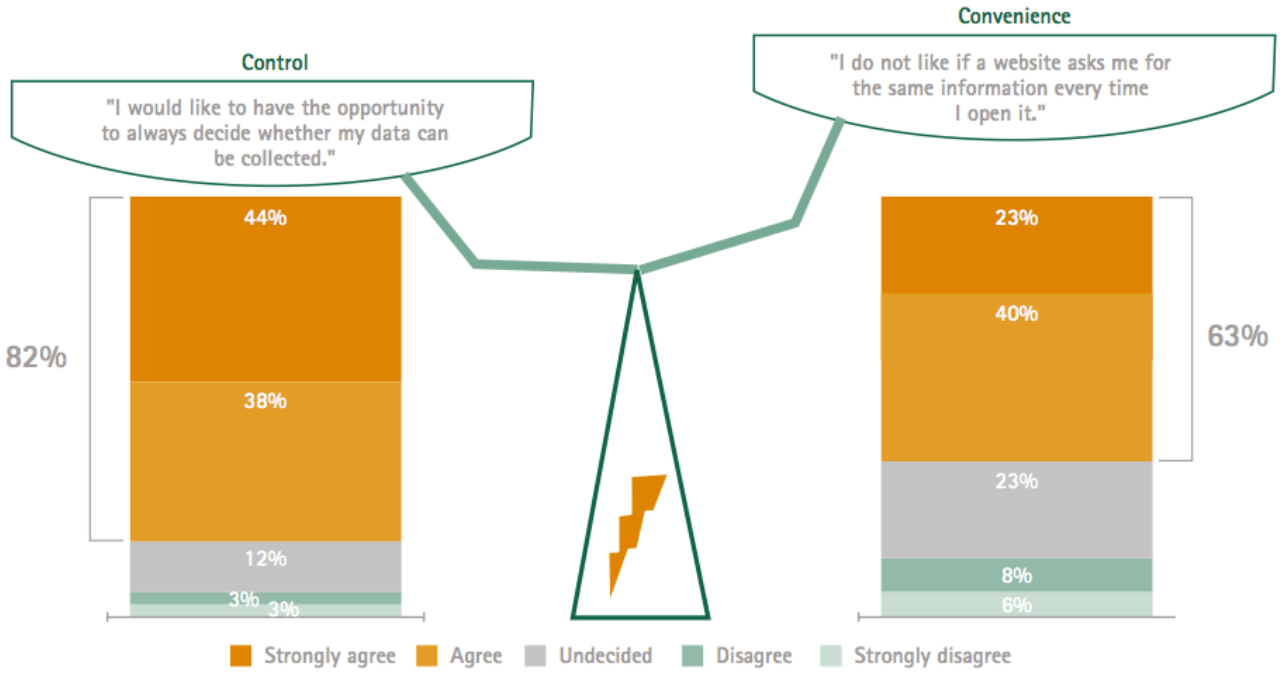
As noted above, individuals have become increasingly concerned about personal data control, privacy, and security online. The media has called the growing concern for privacy, evidenced by surveys and also the acceleration in campaigns, regulatory and legislative measures, and lawsuits in this arena, “The Snowden Effect”[26].

[23] Privacy Rights Clearinghouse, *Chronology of Data Breaches*, 2005.

[24] Mydex CIC, *The Case for Personal Information Empowerment: The rise of the Personal Data Store*, 2010.

[25] Haddadi et al., “Personal Data”, 2015.

[26] Davos, “The Snowden effect”, 2014.



Source: BCG digital identity survey (n = 3,107, August 2012)

Figure 6: The user balance of priorities between control and convenience.

However, a 2012 report conducted by BCG found a contradiction between individuals' stated concerns and their actual behaviour in regard to privacy, control, and convenience[27] (See Figure 6 on Page 10):

> "[M]ost respondents – 82% – expressed the wish to decide for themselves whether to allow data use in each instance. But a majority – 63% – also agreed with the statement, 'I do not like if a website asks me for the same information every time I open it.' Control and convenience are important aims. They are often conflicting aims, too. Balancing them will not be easy – but it will be critical."
>
> *The Boston Consulting Group*

A PDS system could potentially address this behavioural paradox – and the required balancing. The tension between control and convenience might only exist because no viable alternative to the organisation-centric model of data management has been accepted.

One reason the Commission is interested in exploring the PDS concept is as a means to impart individual control over personal data[28]. A PDS system could alleviate trust issues and redress information asymmetries by making data management more user- centric and thus transparent. Privacy is subjective; control enhances privacy because it allows the individual to decide how much to share. In effect, control enables the exercising of the right to privacy.

A well-implemented PDS system could lead to additional individual benefits:

- New forms of remuneration: Various instantiations of the PDS system, as envisioned by current developers, allow users to not only use traditional forms of payment for services, but also allow them to potentially pay with their data – or be paid for use of their data. For example, a third party might request use of a data subject's information for inclusion in a study – the user would then have the capacity to refuse, but should they agree, they could received monetary compensation or use of a

[27] Boston Consulting Group, *The Value of Our Digital Identity*, 2012.

[28] European Commission, *Towards a thriving data-driven economy*, 2014, Brussels. COM(2014) 442 final, p. 11.

service provided by the third party.

- A PDS system could offer convenience in doing away with data silos and unnecessary intermediaries (both online and offline) that individuals must manage piecemeal. Such a PDS system might collate into one manageable space an individual's health data, their financial services information on a range of online accounts, their social media presence on a number of platforms, etc.
- Related to the values of privacy, convenience and control, a PDS system would assist individuals in better collecting, understanding, and more efficiently managing their data; this is particularly relevant as we approach a world of the Internet of Things. A PDS system, if designed with the user's time and attention in mind, might be one solution to a growing problem of information overload[29].
- A PDS system could provide for more personalised services (with consent) due to many third-party service providers having access to a more accurate and rich data pool.

2.2.2 Potential PDS Benefits for Society

A PDS system has the potential to fuel greater DSM engagement – and thus economic growth – by counteracting problems associated with today's organisation-centric data management. Today's system is corrosive to user trust due to privacy, data breaches, unnecessary data retention, and data monetisation concerns. As described above, putting individuals in control of their data allows them to choose the level and conditions of their data dissemination.

In addition to potentially increasing trust in online transactions, a PDS ecosystem would lower costs, increase efficiency for service providers, and stimulate the provision of more services, for the following reasons:

- Providers have certain economic incentives to develop services - this arises from the proliferation of cost savings to public and private providers in terms of increased efficiency and economies of scale, inherent in cloud-based technologies and big data[30]. This is a particularly salient point for small companies, who find data processing increasingly expensive – despite lowering hardware and cloud computing costs. This is due to excessive duplication, error, and general inaccuracies, and especially for small firms, the high cost of data acquisition is beyond their limited user base.
- If a PDS system were implemented in a way to allow providers to easily base data transfer on consent (perhaps even in an automated fashion), this could cut down on compliance overhead and allow providers to more easily expand into different regulatory regimes.
- A PDS system will allow providers to make use of cleaner, richer, safer, and easily accessible data 'as input into new types of personalized services'[31].

Over time, a PDS ecosystem could also potentially facilitate the consent needed for collection of and analytics on personal information. Big data – fast becoming a ubiquitous term in innovation reports and technology policy briefs – refers to significant and continuing advances in the volume, variety, and velocity of data analysis[32].

Health Case Study — Big Data Analytics
Big data analytics could be used to forecast and track health conditions (e.g., potentially affecting insurance premiums in private healthcare systems such as those in the US) or facilitate targeting of consumers based on sensitive personal aspects (such as financial condition or addictions)[33,34,35]. ■

Many significant privacy and control issues related to big data have arisen as the world becomes increasingly connected, and as information is continually managed in an organisation-centric manner[36]. Thus, one

[29] Hudson, "The age of information overload", 2012.
[30] Podesta et al., *Big Data: Seizing Opportunities, Preserving Values*, 2014.
[31] Mydex CIC, *The Case for Personal Information Empowerment: The rise of the Personal Data Store*, 2010.
[32] OECD, *Data Driven Innovation for Growth and Well-being*, 2014.
[33] Brill, "Big Data and Consumer Privacy: Identifying Challenges, Finding Solutions", 2014.
[34] Walker, *Data Mining to Recruit Sick People*, 2013.
[35] Mydex CIC, *The Case for Personal Information Empowerment: The rise of the Personal Data Store*, 2010.
[36] Mydex CIC, *The Case for Personal Information Empowerment: The rise of the Personal Data Store*, 2010.

benefit of a PDS system is the potential alleviation of such data protection and privacy concerns, given that the user is at the heart of the data management. For example, researchers could ask individuals directly for access to their data, rather than relying on preexisting datasets.

Also related to data collection and analysis, a PDS system could be of great significance to smaller organisations who struggle to obtain sufficient quantities of relevant data or successfully extract value from that data, which slows innovation and growth at the firm level as well as in the broader economic sense. From the public sector perspective, movements towards open data combined with big data analytics can provide insights and opportunities for growth. As various administrations move towards "unleashing troves of valuable data that were previously hard to access", they facilitate innovation and insight in a wide variety of domains: health, energy, climate, education, public safety, finance, and global development[37]. The insights cultivated from big data, and particularly via the opening of these kinds of data sets, can lead to[38]:

> [...] profound benefits by addressing important societal issues like keeping kids in high school; conserving our natural resources by making our use of electricity more efficient; providing first responders in crisis situations with real-time information about the injured or those who lack power, water, or food; and performing other miracles in the healthcare sector.
>
> *Julie Brill*

2.2.3 Social Concerns For a PDS System

The rise of PDS services will depend on whether such a widespread platform is flexible, robust, and trusted enough to realise an enormous heterogeneity in users, uses, and attitudes. It will also depend on whether providers can alleviate the privacy and control concerns inherent in any aggregation or centralisation of data, even if just via an interface. Creation of such a platform and environment poses significant social barriers– and this is one major reason why no PDS system has had widespread success in the market as of yet, for user-centric apps or for big data analytics[39].

If providers do not take into account values of convenience in PDS construction, the PDS could very well overwhelm the user[40]. For example, if a PDS floods a user with consent requests, prohibitively complicated and extensive terms of service, and minute management requirements, the user is 1) less likely to utilise the system and 2) less likely, if using the system, to fully control data or understand the purposes for which it is being collected. Such a state of affairs is only a replication of many current issues in data management practices, and would potentially detract from the benefits to users – thus underlining the need for continual consideration of the user in design of any PDS system (See Section 4.5 on Page 39). In fact, a PDS system could be one way to address rather than aggravate an ongoing problem of information overload; machine-readable technologies could enable a situation where users' preferences are embedded into the actual architecture of the system (See Section 3.5 on Page 25).

The PDS system, with its user-centric design, is a potential solution to privacy issues in current data management practices, but it also poses the risk of aggravating those issues as it eases friction in data transfer and analytics. For example, big data not only poses some of the biggest opportunities in terms of research, delivery, and governance, but also some of the biggest privacy risks.

The privacy concerns surrounding big data allow for insights and predictions that can deeply affect individuals, especially if they do not have any sort of control over their data. The 'mosaic effect' of big data – where disparate, seemingly unrelated data points can be combined to identify a consumer – allows organisations to turn 'anonymous' data into 'identification' data[41,42]. Additionally, big data can allow the creation

[37] Podesta et al., *Big Data: Seizing Opportunities, Preserving Values*, 2014.
[38] Brill, "Big Data and Consumer Privacy: Identifying Challenges, Finding Solutions", 2014.
[39] Haddadi et al., "Personal Data", 2015.
[40] Boston Consulting Group, *The Value of Our Digital Identity*, 2012.
[41] Wittes, *Database*, 2011.
[42] Podesta et al., *Big Data: Seizing Opportunities, Preserving Values*, 2014.

of ever-more detailed, predictive profiles that could foreseeably infringe on the privacy rights of consumers.

Health Case Study — Social Aspects
The health sector stands to gain the most from a PDS system, but it also faces some of the biggest hurdles[43]. Not only is health data one of the most sensitive types of personal data, both in law and practice, but healthcare in the EU is under the purview of Member States – and thus difficulties of creating cross-border services are amplified[44].

PDSs offer individuals numerous benefits. For example, a PDS system could provide access to medical records – and such access "promotes patients' participation in their own care"[45]. Not only would participation increase with improved access and control, but preventative efforts would become more effective and efficient – on the sides of both the healthcare provider and the consumer[46]. This participation could take the form of greater awareness and individual initiative, but also potentially in the provision of new health services and products that such an innovative platform could incentivise. Richer and cleaner datasets, the possibilities for analytics, the provision of new and better targeted services–all aspects could contribute substantially to higher quality healthcare. Care could be also become increasingly personalised as richer data sets are created; individuals could thus receive more accurate diagnosis and treatment. For a case study from Luton Dunstable hospital in the UK, see Section 4.9.1 on Page 48.

A PDS system could facilitate overall lower costs for healthcare systems via more targeted, preventive, and engaged care. This reduction could be further augmented should a PDS encourage greater expansion of electronic healthcare systems. This would occur via increased efficiency from consolidation of paper trails and data silos often found in the health system via the creation of an electronic healthcare system. For example, one national survey in the US found that, "based on the size of a health system and the scope of their implementation, benefits [of EHRs] for large hospitals can range from $37M to $59M over a five-year period in addition to incentive payments"[47]. These cost savings arise primarily from automating 'labor-intensive' and 'paper-driven' tasks, including reduction of medical errors due to quick and easy access to patient data, reducing costs of chart management, and improved care through greater patient education, among others.

But one of the biggest societal benefits that could arise from a PDS system - if it were to facilitate more big data analysis of health data - would be through greater research capabilities enabling faster scientific and medical advances as well as new research into previously data poor areas such as rare diseases. The examples are already astounding – from predicting outbreaks of dengue fever and malaria to preventing tuberculosis[48].

However, a health-focused PDS will need to navigate a number of difficulties, particularly in the realm of privacy and data protection. Health data is seen as some of the most sensitive by both individuals and the law – it is subject to more concern, more risk, and more regulatory protections. As noted in various studies, consumers are more concerned about sharing their health data than other types of personal data[49]. This is partially because health records contain a plethora of important data: personal, financial, and medical. According to a survey conducted on US consumers, most prioritise health data security over more convenient services (See Figure 7[50] on Page 14). Any personal data store dealing with health data, therefore, must be able to prove its ability to store or access individual's health data securely in order to gain the market's trust. This does however suggest that a viable entry point for a PDS is in the healthcare sector where consumers already indicate that more control is desired even if it means less convenience.

■

[43] W. Raghupathi and V. Raghupathi, "Big data analytics in healthcare", 2014, p. 3.

[44] Progress Consulting S.r.l. and Living Prospects Ltd., *The management of health systems*, 2012, Commissioned Study. Brussels: European Union.

[45] OECD, *Data Driven Innovation for Growth and Well-being*, 2014.

[46] Brill, "Big Data and Consumer Privacy: Identifying Challenges, Finding Solutions", 2014.

[47] Bell and Thornton, "From promise to reality", 2011, pp. 50–56.

[48] Grant, *The promise of big data*, 2012.

[49] PwC, *Issue 3: Balancing privacy and convenience*, 2015.

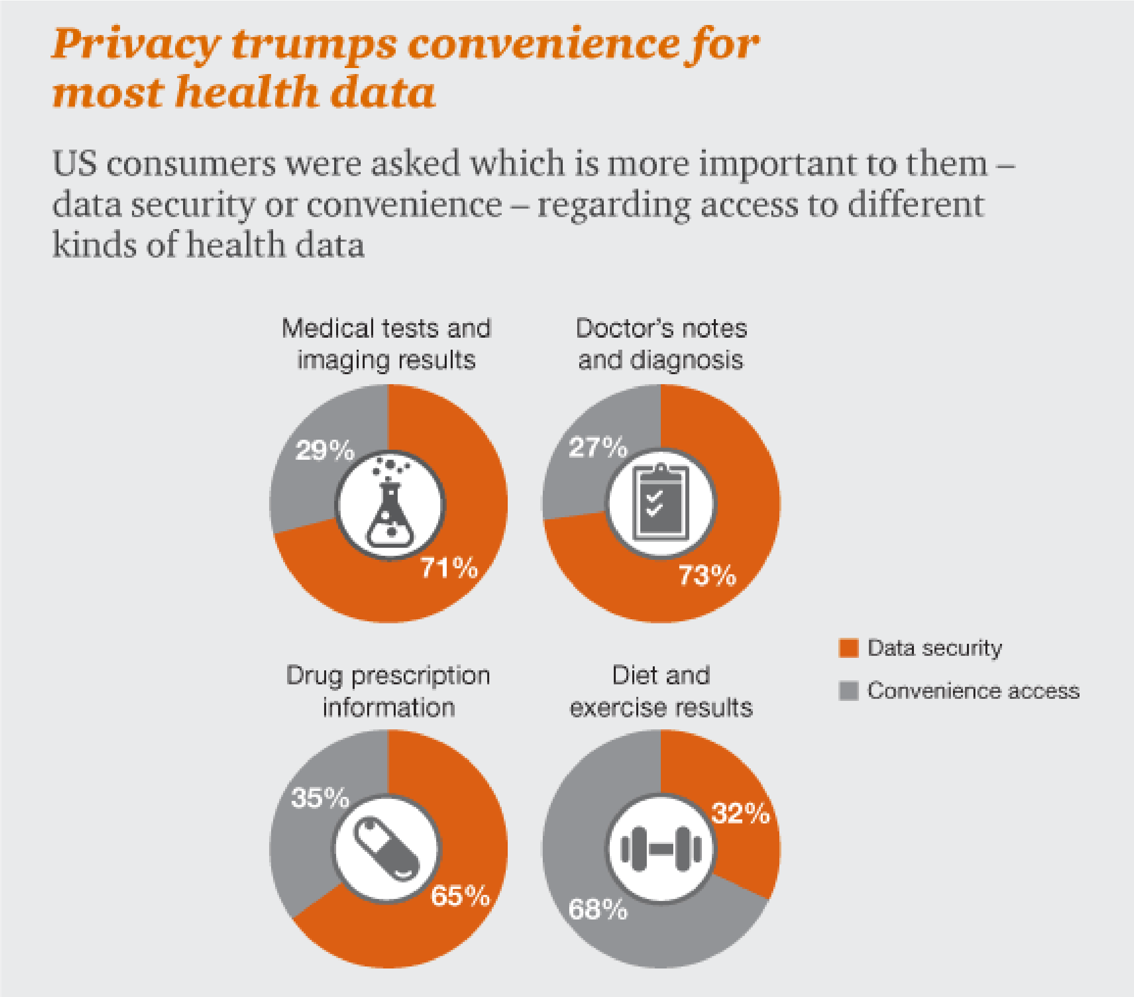


Figure 7: US consumers were asked which is more important to them – data security or convenience – regarding access to different kinds of health data. Results indicated that privacy trumps convenience for most types of health data

2.3 Legal Considerations for a PDS System

2.3.1 Regulatory Environment and Requirements for PDS Providers

With the rise of the information economy, there is a heightened need to update regulation to reflect reality – not only to provide for the protection of users' rights but to facilitate the functioning of a knowledge-based economy. This is one reason why the creation of the Digital Single Market is one of the top priorities of the Juncker Commission. Fragmentation of regulation constitutes barriers to the free flow of information and services – preventing the existence of a frictionless pan-EU digital economy[51,52]. For example, the development of a successful PDS system that would stretch across more than one Member State is made more difficult by Member States' differing transpositions of data protection law. This manifests in different requirements for notification, consent, localisation of data, etc. Such fragmentation hinders potential economic growth and innovation by creating barriers for organisations to expand.

Any PDS business operating within the EU would be subject to significant requirements to maintain compliance with existing data protection laws. This is one reason why several PDS developers have devoted considerable resources to creating legally compliant technical framework for adequate compliance[53]. EU legislators are in the process of updating data protection laws through the proposed data protection regulation. The current data protection directive was implemented in 1995; since then, in its proposal released in January of 2012, the EC has indicated that rapid technological advances have brought new challenges, transforming the economy and social life[54]. The proposal also documented that building user trust is key to further economic development, concluding that the EU needs a more comprehensive and coherent policy on the fundamental right to personal data protection. However, as of now, fragmentation between Member States' regulatory regimes (based on transposition of the current Directive and perhaps the derogations allowed in the new regulation) remains, and the hurdles for compliance (e.g., different data localisation requirements in different Member States) are burdensome. Below is a brief overview of the legal context in which a PDS would thus operate, legal bases for its operation, some of the barriers it would face, and how it could potentially facilitate better compliance with EU regulatory aims.

Personal data under EU law is linked to identity; any information that is "relating to an identified or identifiable natural person ('data subject')" is subject to significant and specific conditions for legitimate, lawful processing. Processing is a broad term, referring to collection, recording, organisation, storage, and other activities surrounding data management. Certain types of personal data are subject to even stricter conditions – this special class of data is called 'sensitive data', and it includes data relating to race, politics, religious beliefs, and health, among others[55].

Health Case Study — Classification and Treatment of Health Data
Health data is classified as sensitive under current law, which means that processing of such data is subject to higher levels of data protection. But in addition to this qualification, there is the added complication of discerning what kinds and collations are health data. For example, medical related data – or that "[...] about the physical or mental health status of a data subject that are generated in a professional, medical context" – are uniformly and undisputedly classified as health data under data protection[56]. But there are other types of data (e.g., generated by health monitoring apps, relating to a subject's emotional or intellectual capacity, pertaining to membership of support groups) that can fall under the much broader term 'health data'. This is an area that needs further guidance from regulatory authorities. Thus, the European Data Protection Service published an opinion with guidance on classification of mobile health data[57]; additionally, the Article 29 Working Party provided some guidance on the topic in response to a EC request for clarification[58]. ■

[50] PwC, *Issue 3: Balancing privacy and convenience*, 2015.
[51] Commission, *Data Protection Day 2015: Concluding the EU Data Protection Reform essential for the Digital Single Market*, 2015.
[52] Commission, *A Digital Single Market Strategy for Europe*, 2015.
[53] Respect Network, *Respect Trust Framework* .
[54] European Commission, *General Data Protection Regulation*, 2012.
[55] European Commission, *General Data Protection Regulation*, 2012, art. 9, pg. 45.

Entities involved in processing of personal data must respect the rights of data subjects while conducting their processing activities. These rights, as also laid out in the data protection directive, include: the right to be informed, to access data, right to erasure, right to restrict, and data portability. With an organisation-centric model of data management, giving these rights the accordance they require can be almost unrealistic in today's high volume data transfer environment – as has been noted by regulators as well as industry[59].

Whatever the case, compliance with current data protection law for any PDS system that wishes to serve users across borders will include several challenges. Data protection law in the EU is in the process of being updated, with adoption and enforcement being predicted in the next few years. Below are several elements from the current proposal which are particularly relevant to PDS development[60].

- Article 3 refers to territorial scope: the Regulation applies to controllers within but also outside the EU if they provide services in the EU or monitor EU citizens. This is especially relevant in the case of cloud computing services; the architecture of a PDS, particularly if developed by cost-conscious SMEs in other jurisdictions, would almost certainly include cloud storage (See Section 3.3 on Page 22).
- Article 5 lays out general principles that should apply to processing, building on the Directive's Article 6 (i.e., data must be processed lawfully, collected for a specific, explicit, legitimate purpose, must be relevant and not excessive, accurate and up to date, etc.). The Regulation includes additional requirements for transparency and adherence to the data minimisation principle; a minimal amount of personal data must be collected in order to fulfil the purpose of processing. Additionally, it must be understood by the PDS provider the extent of "the establishment of a comprehensive responsibility and liability of the controller".
- Article 6 sets out lawfulness of processing, particularly with regard to balancing of interests (e.g., private and public).
- Article 7 "clarifies the conditions for consent to be valid as legal ground for lawful processing". This is particularly relevant to a PDS system, as most likely its processing would be based on consent rather than alternative conditions such as contract.
- Article 9 "sets out the general prohibition for processing special categories of personal data [the sensitive data] and the exceptions from this general rule, building on Article 8 of the Directive 95". This is especially pertinent for any health-based PDS, as the majority of the data being processed would be sensitive.
- Article 17 on the right to erasure and Article 18 on right to data portability are particularly relevant to a PDS provider, and to any public entity trying to facilitate adoption of a PDS, because a user-centric data management model could allow for the full and informed exercising of these rights in an unprecedented manner; the current state of affairs - organisation-centric management of personal data - creates a system of burdensome requirements and opaque mechanisms for the data subject if they wish to move their data en masse to a new platform or erase their data based on its inaccuracy, irrelevancy, inadequacy, or excessive nature. However, if such rights are to be exercised fully, interoperability between systems is essential. (See Section 3.4 on Page 23).

[56] Article 29 Working Party, *Annex: Health Data in Apps and Devices*, 2015.

[57] EDPS, *Mobile Health: Reconciling Technological Innovation with Data Protection*, 2015.

[58] Article 29 Working Party, *Annex: Health Data in Apps and Devices*, 2015.

[59] Robinson et al., *Review of the EU Data Protection: Summary*, 2009.

[60] Parliament, *GDPR - Draft*, 2014.

Health Case Study — Complexity of Compliance in the Health Sector
PDS providers looking to create a service around the control of health data in the EU must be able to create a system that is compliant with processing requirements for sensitive data, but also flexible enough to address the diversity of health data types, healthcare systems, and contexts of access.

A PDS system could be used to further individuals' rights to access and control their health data, and not just under data protection law. As noted above, this is particularly relevant to the general rights of portability and to erasure. But additionally, under Directive 2011/24 on Patients' Rights[61], citizens have the right to obtain copies of and maintain ongoing access to their health records (Article 4F)[62]. Thus, a PDS system would ideally need to partner with the controlling organisation over health records (e.g., hospitals, individual healthcare providers, or municipalities) as well as the individual. Such a partnership would ensure that data was accurate and updated; it would also allow for flexibility in situations where health data needed to be quickly and easily accessed by third parties, as in an emergency.

The conditions for partnering and flexibility in access would vary, depending on the Member State's healthcare system and data protection laws. For example, the conditions for third-party access to health data, in the vital interest of the data subject, would depend on how a Member State transposed this portion of the Directive. Additionally, the controlling organisation over healthcare records might by a municipality (as in Holland) or a national program (as in the UK). ■

2.3.2 Legal Basis and Challenges for a PDS System

The most likely legal basis for the PDS system would be one based on consent – explicit and informed – especially if the PDS system is processing sensitive data as defined in Article 9[63]. However, there is a possibility of a contract offering a legal basis in the context of ordinary personal data processing as defined in Article 7[64]. As such, consent within the framework of a contractual relationship would be satisfactory if (1) the processing must be necessary for the performance of the contract and (2) the processing for the contract is sufficient to justify any necessary correlated processing. Thus, from the perspective of the developer and the user, consent is not as straight forward a requirement as it might seem and introduces complexity for both sides, possibly affecting the value proposition.

- As noted in Section 2.2.3 (See Page 12) users sometimes have competing values of privacy and convenience; a PDS system that bombards its data subjects with constant notices and requests may be a harder sell to consumers and detrimentally affect long-term user retention.
- There are situations when informed, explicit consent cannot realistically be given for future use – this is especially true in the case of big data analytics, particularly in the case of scientific research. The concept of 'broad consent' has been put forward as a solution to this state of affairs. For example, in the context of biobanks, users give 'broad consent' for the use of their data though not all of the specifics about particular uses of samples are available. This is justified by the potential benefits that might arise from this research, as well as the assurance of a low level of risk to any privacy or confidentiality breach[65]. However, it remains a point of unresolved contention if such a concept is fully compatible with the objective of EU data protection regulation – where the user must be fully informed – and if it could be employed in a PDS context.
- Building into the system abilities (both automatic and manual) to withdraw consent, to identify or classify data by type (personal, sensitive, and its manner of collection) or to automatically 'forget' irrelevant, inadequate, excessive, or inaccurate data – all of these represent significant compliance complications that PDS developers face[66].

[61] European Parliament and Council, "DIRECTIVE 2011/24/EU", 2011.

[62] European Parliament and Council, "DIRECTIVE 2011/24/EU", 2011, Article 4(f), pg. 56.

[63] European Commission, *General Data Protection Regulation*, 2012, art. 9, pg. 45.

[64] European Commission, *General Data Protection Regulation*, 2012, art. 7, pg. 45.

[65] Sheehan, "Can Broad Consent be Informed Consent?", 2011, pp. 226–235.

[66] Haddadi et al., "Personal Data", 2015.

Challenges

In addition to the above requirements for compliance, PDS providers in the EU face a patchwork of regulatory regimes, meaning that they would have to readjust their schemes for reporting, notices, and requests to fit the different versions of the Directive transposed in each regime. According to some interviewees, this patchwork of regulatory regimes has caused current PDS-like providers to delay expansion into other Member States. One of the aims of GDPR is to rectify this situation by harmonising requirements across the EU, and facilitate easier cross-border transfers by measures such as the 'One Stop Shop Principle', as laid out in Chapters VI and VII of the current proposed regulation[67]. The aim of the One Stop Shop principle is to cut down on administrative overhead (for both companies and regulatory agencies) by allowing companies to receive single supervisory decisions regarding cross-border data flows, rather than multiple decisions concerning multiple regulatory regimes. The proposed regulation should also create a more favourable environment for SMEs operating in this space due to the reduction in administrative overhead resulting from compliance. The Commission has proposed to exempt SMEs from several provisions of the Data Protection Regulation[68]. Under the new rules, SMEs would benefit from four reductions in red tape:

- **Data Protection Officers:** SMEs are exempt from the obligation to appoint a data protection officer insofar as data processing is not their core business activity.
- **No more notifications:** Notifications to supervisory authorities are a formality and red tape that represents a cost for business of €130 million every year. The reform will do away with these requirements.
- **Every penny counts:** Where requests to access data are excessive or repetitive, SMEs will be able to charge a fee for providing access.
- **Impact Assessments:** SMEs will have no obligation to carry out an impact assessment unless there is a specific risk.

Health Case Study — Different Regulatory Regimes: Health and Data Protection
PDS providers who are operating in a health data context must also navigate the different healthcare systems of Member States. Article 168 of the Treaty of the Functioning of the EU notes that organisation and delivery of health services and medical care – the management of the health systems – falls under the competence of the Member States.

This manifests itself in a wide diversity of healthcare systems across the 28 Member States. The magnitude of differences has prompted the creation of EU-level monitoring programs[69] (EUCOMP 1 and 2) to continually assess differences between organisations and funding of each member state's healthcare system. This is one reason why certain SMEs – those that have established services with specific hospitals and municipalities in a member state, and tailored their compliance and products accordingly – have struggled to expand to other Member States. ■

2.4 Conclusion

This section explored current and potential aspects of the larger socio-legal context surrounding a PDS system. This was done via examination of possible benefits and concerns surrounding PDS development from multiple perspectives: individuals (data subjects), the PDS providers, the policy makers, and society at large.

For individuals, a PDS could provide values such as enhanced control of personal data without subtracting from convenience of digital profile management; a better means to exercise a range of information-related rights; and provision of a range of new services and means of remuneration for the same. If such values are realised on an individual level and uptake is sufficient, the PDS system could impart greater benefits to society at large. For example, a fully-fledged PDS system would potentially increase engagement in the Digital Single Market, create a new platform for innovation, and provide new venues for big-data based

[67] Council of the EU, *Data protection: Council agrees on general principles and the "one stop shop" mechanism - Consilium*, 2015.
[68] Commission, *Data Protection Day 2015: Concluding the EU Data Protection Reform essential for the Digital Single Market*, 2015.
[69] European Commission, *Comparing the organisation of health systems, Health Systems Performance Assessment* .

research.

But the PDS concept is not without its challenges – barriers to development range from current limited market reach (related to consumer perceptions of privacy and security risks inherent in data aggregation as well as general lack of information disseminated about such systems) to the disparate regulatory regimes with which providers must contend in developing platforms. Thus, the paragraphs above also explored the PDS concept from the view of the provider and the various regulatory compliances and design decisions that should be taken into consideration.

The health sector stands the most to gain from a PDS system, but it also faces some of the biggest challenges in development. Health data, classified as sensitive and thus subject to even more stringent requirements for processing, is also the data that individuals are most reluctant to share. Additionally, providers face significant challenges in creating interoperability between not only disparate data protection regulatory regimes but also healthcare systems. But the values that a health PDS system could impart to both individuals and society at large is significant: from better tailored medical care to lowered healthcare costs on all levels to medical advances from better analytics.

By examining the socio-legal benefits and concerns surrounding the PDS from these multivariate perspectives, especially in regard to a health-focused PDS, the EC or any similar body looking to facilitate development and adoption of PDSs can 1) determine if PDSs are a viable mechanism to facilitate access to data, consumer trust, popularity of the DSM, etc., and 2) decide which policy measures and resource allocation are most appropriate.

3. Technical Considerations

3.1 Introduction

A key question arising in the context of facilitating the PDS concept is whether the technical capability currently exists to enable broader PDS adoption This section explores existing technical formats, standards, and architectures relevant to the PDS ecosystem; this is especially important in the case of the healthcare sector, because interoperability of data is essential for the realisation of big data benefits and cross-border continuity of care, but where the EC does not currently have the mandate to enforce this interoperability[70].

However, the EC could issue, or facilitate and support the issuing of guidance documents on best practices concerning interoperable standards, data formats, and architecture, as well as privacy by design to facilitate PDS ecosystem growth; the EC could also work to alleviate the coordination problem inherent to emerging innovations by acting as a central point of contact and coordination for industry development of interoperability and technical standards. Under Article 168, the Commission "may [...] take any useful initiative to promote such coordination, in particular initiatives aiming at the establishment of guidelines and indicators, the organisation of exchange of best practice, and the preparation of the necessary elements for periodic monitoring and evaluation."[71]

3.2 Conceptual PDS Architecture

There are currently several different architectural implementations possible for PDS. A key question is: how could these different technical features encourage or discourage the PDS market and user adoption? Architectural implementations of PDSs will either be (1) cloud-based storage, or (2) local storage (e.g., on a mobile phone), which each entail their own security and cost implications. Cloud-based systems will likely hold encrypted data behind web and authentication layers (See Figure 8 on Page 21), while on-premise/local systems will store data on a user's device in encrypted form accessible via Application Programming Interface (API) calls through the PDS application layers. API layers act as a common access point to web-based technologies for third-party developers to interface with a proprietary system. If the data is stored locally on an iPhone for example, developers will have to interface through Apple's API to access the locally stored data. Either deployment will involve layers of encryption, key management and authentication layers but will be employed by either the local hardware provider, or the PDS provider, or both, depending on the specifics of the architectural implementation.

Figure 8[72] on Page 21 demonstrates graphically – at a high level – two possible architectural implementations of the PDS concept, (1) cloud based, and (2) local storage. On the left of the diagram, the user interfaces with the API access layers through their preferred mobile or desktop device. Various protocols would be implemented at this step for procurement and handling of data transmission, login credentials, encryption and decryption key handling, and various levels of service request through the PDS provider. The cloud-based infrastructure layer which consists of Software, Platform and Infrastructure as a service (SaaS, PaaS and IaaS) allows for a common access point from either side of the ecosystem (for developers and third-party services on one side, and for the user on the other side)

[70] *Consolidated Version of the Treaty on the Functioning of the European Union*, art. 168, 2008 O.J. C 115/47.

[71] *Consolidated Version of the Treaty on the Functioning of the European Union*, art. 168, 2008 O.J. C 115/47.

[72] Eisma, *PDS Conceptual Architecture*, 2015.

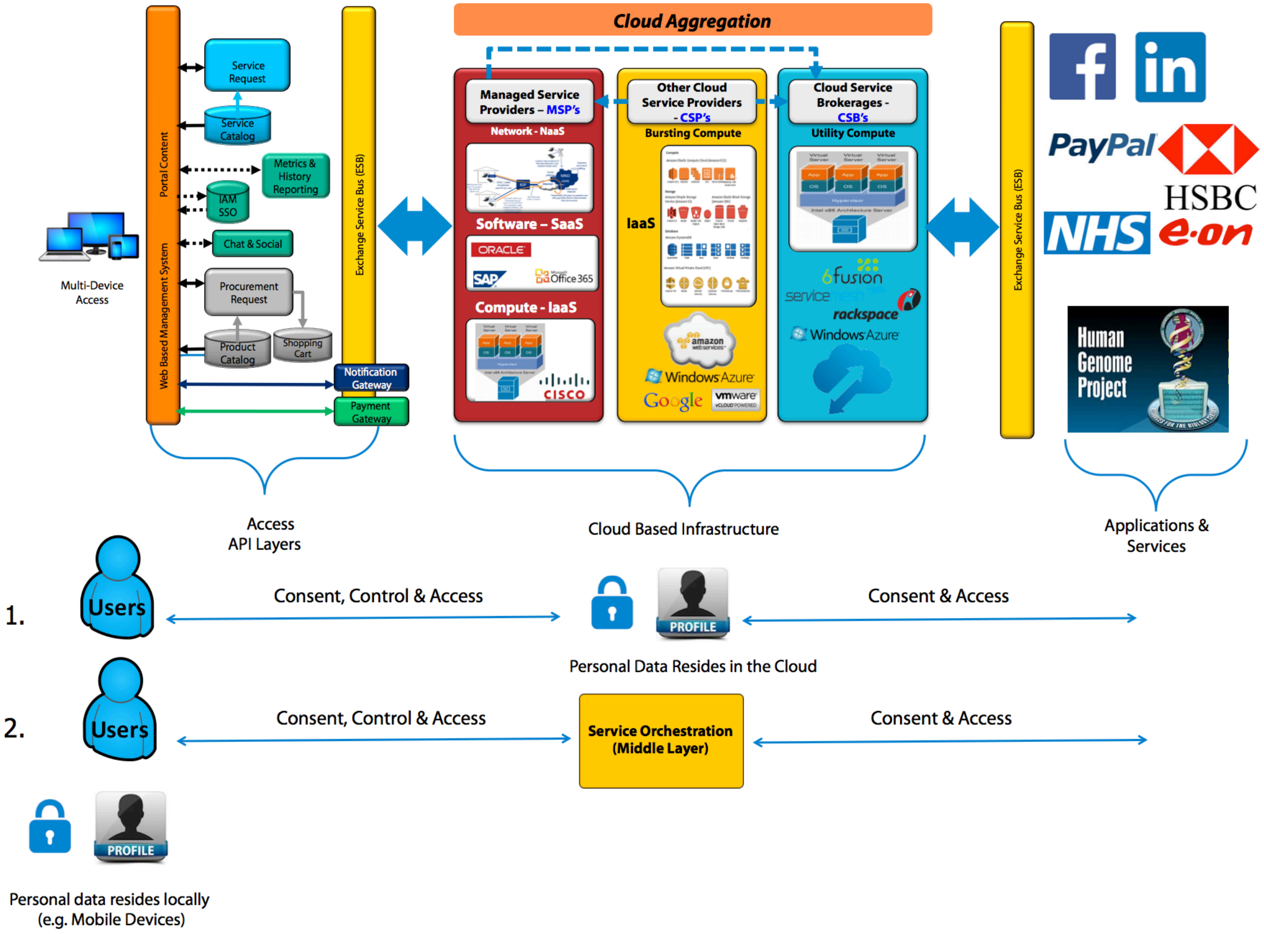


Figure 8: Architectural implementations of the PDS concept highlighting two different approaches of storing personal data, (1) cloud based and (2) local storage. On the left of the diagram, the user interfaces with the API access layers through their preferred mobile or desktop device. Various protocols would be implemented at this step for procurement and handling of data transmission, login credentials, encryption and decryption key handling, and various levels of service request through the PDS provider. The cloud-based infrastructure layer which consists of Software, Platform and Infrastructure as a service (SaaS, PaaS and IaaS) allows for a common access point from either side of the ecosystem (for developers and third-party services on one side, and for the user on the other side)

3.3 Security

With cloud-based storage, an ideal security situation is one in which the data and the key to access it are separated, e.g., the individual holds the decryption key on their mobile device and the cloud service provider holds the data. In this system, even if hackers obtain the key through malicious access to the individual's mobile device, they still cannot access the data on the cloud service providers without the user's login credentials for the PDS service. It would seem that remote storage of the key would be better in this circumstance; however, this would create a situation where any malicious access to the cloud-based storage would provide the hacker with both the data and the key to decrypt it. With local storage of the key this risk is mitigated, however, there is still a risk with local storage of keys if the attacker gains the user's login credentials. However, physical separation of the key and the data is considered essential for security. It is possible that a new firm operating as a third-party verification service could hold the keys separate from both the individual and the PDS provider to provide an additional layer of security (Such a scenario is considered in Figure 10 on Page 27). In either case, with separation of the data from the key in this system, if the hacker breaches the cloud service provider's defences, the data remains encrypted. Another benefit of such an architecture is that cloud service provider employees cannot access individuals' unencrypted data.

More technically, with this type of cloud-based storage (and local or third-party storage of decryption keys), since there is both physical and architectural separation between the data and the means of decryption, the loss or theft of a device containing the keys or the hacking of the cloud service are each insufficient to allow for access to the data. Some SME providers (such as Digi.me) have been operating under a local-storage paradigm in an effort to reduce cloud-based storage costs. However, with local storage, mobile phones and similar devices are often protected by nothing more than a simple short password. While on-device data may be encrypted, unless there is physical separation of the private keys - as described above - once a user with malicious intent has access to the physical device, they may obtain all of the information contained therein. A solution to this is again physical and architectural separation of the data where the storage of decryption keys could be with the PDS provider or a third party verification service. Combining all of these aspects of a PDS architecture - the security concerns, economies of scale and the standardised storage and encryption possibilities, and the need to guarantee timely and equivalent access to data for third parties such as hospitals and researchers - it is recommended that a cloud-based storage solution be implemented, though user-perception of storage architecture remains unexplored and may be an important factor.

While alleviating security risks at the individual level, cloud-based storage still creates the perception that there is raised risk. Due to the centralisation of data (either physically or through a common interface), there are greater security risks should a data breach occur, as an individual or group with malicious intent has access to a larger set of data from many users. Cloud-based data storage, with the encryption keys stored locally on users' devices, or with a trusted third party as described above, offers benefits of both cloud-based and local-storage solutions while mitigating this perceived large data set risk. However, one aspect which requires further study is user attitudes towards various data storage architectures and the impact this has on trust and service usage since local storage may often seem safer to users. An effective educational and marketing strategy would be essential to overcome this potential barrier.

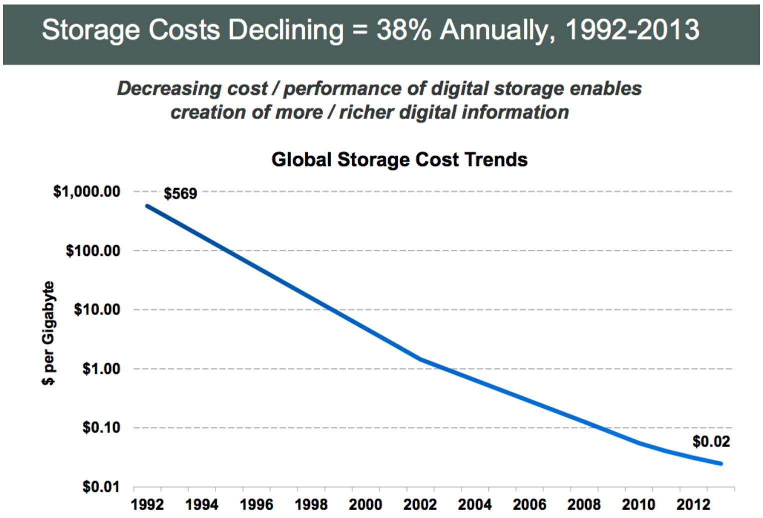


Figure 9: Cloud storage costs continue to decline

3.3.1 Potential Tradeoffs Between Security and Cost

The security architecture described in Section 3.3 (Page 22) should not imply significant expense for the PDS provider, as hardware storage costs are rapidly falling[73,74] (See Figure 9[75] on Page 23).

Intuitively, the more layers of security that are provided, the higher the cost to the implementing organisation. Typically this means that for organisations where the potential risk of a data breach is low, security is implemented at a level of minimum compliance. However, as the primary value propositions for the PDS concept are enhanced data protection, privacy, and control of personal information, the risk of a data breach to both the user and the business is high. It is thus expected that PDS SMEs will have to expend higher-than-average costs to ensure a proportionate security system is in place, but that this is a necessary part of the value proposition. The concept was summarised by Fraser[76]:

> " One old truism in security is that the cost of protecting yourself against a threat should be less than the cost of recovering if the threat were to strike you. Cost in this context should be remembered to include losses expressed in real currency, reputation, trustworthiness, and other less obvious measures. "
>
> *Fraser*

3.4 Interoperability

Interoperability is envisaged as an essential feature of a fully functioning PDS ecosystem. The concept can refer to functions on multiple levels of the PDS architecture, such as: data formats, data exchange protocols, semantic interoperability, or data portability. Consistency in data storage formats and exchange protocols would allow for the simplest implementation of an interoperable system, with semantic interoperability based upon an extensible markup language (XML) facilitating easier information processing. An essential value proposition for an interoperable framework is that it also grants the user easier ability to exercise their right to data portability. According to its general definition[77]:

[73] Rubens, *Can Cloud Storage Costs Fall to Zero? - EnterpriseStorageForum.com*, 2014.
[74] Millman, *Google price cuts see cloud costs fall by 10 per cent | Cloud Pro*, 2014.
[75] Business Intelligence, *Cloud Storage Costs - BI Insight*, 2014.
[76] Fraser, *Site Security Handbook*, 1997.
[77] Aliprandi, "Interoperability and open standards", 2011, pp. 5–24.

> “[...] interoperability is the intentional design of a technology product or system, which allows it to cooperate with other products or systems without restriction or difficulty, thus producing a reliable outcome and resource optimization. The main goal of an interoperable system is to facilitate interaction between different software applications and to enable sharing and re-use of information among non-homogenous systems.”
>
> *Simone Aliprandi*

One of the long-term requirements for a fully competitive PDS ecosystem, and one which allows for data portability at low cost (maximising user choice), is interoperability of data between PDS providers[78]. In the early stages of an emerging PDS ecosystem, it is hypothesised that there is an economic incentive to maximising interoperability between PDS providers; until a critical mass of users is attained, there will be lowered incentives for third-party services to interface with the PDS. It is suspected that these third party service providers (such as SMEs wanting to improve the functionality of their online services or products, or take advantage of big data analytics) would be more likely to interface with a small PDS provider if the resources they expend to ensure interaction with the PDS data is transferrable to other PDS providers, thus maximising utility. As described above, this could be obtained through the use of standard API protocols and a common data language such as an XML-based storage format. The RESPECT network, one of the aspiring PDS providers interviewed for this report, has developed such a storage format and an interchange language, termed XDI (See Section 3.5 on Page 25).

Long-term however, there are generally two barriers to interoperability in any industry: the first is a coordination problem, where organisations must effectively network within a diverse field of other competing organisations and agree on standards, and the second is one of misaligned incentives. With misaligned incentives, once an organisation begins to have a self-sustaining product ecosystem and user base, the incentives for interoperability disappear and are replaced with incentives for monopolisation. Ensuring interoperability at the early stages of an emerging industry might be one way to alleviate this concern. Particularly for PDS providers in the health-care space, there are already additional incentives for interoperability due to the necessity of continuity of care across geographical areas and various specialists, and there are already emerging industry standards for data such as HL7.

Currently, several standard methods allow for third party information exchange without sharing user passwords. Google, Amazon and Facebook, for example, use OAuth, which provides a reference architecture for authentication[79,80,81]. PDS providers could use existing standards like OAuth to provide a consistent API framework and interface for developers. It could also facilitate information exchange in a PDS ecosystem, allowing developers to access a diversity of PDS providers, third-party services, and SMEs.

[78] Yaraghi, *A Sustainable Business Model for Health Information Exchange Platforms*, 2015.

[79] OAuth, *An open protocol to allow secure authorization* .

[80] Twitter, *OAuth: Using OAuth*, 2015.

[81] Google, *Using OAuth 2.0 to Access Google APIs*, 2015.

Health Case Study

Healthcare industry-specific standards such as Health Level Seven (HL7) provide a framework for electronic healthcare records exchange and has been widely adopted in the US and parts of the Europe. The standard was promoted by a US non-profit standards organisation and approved by both ISO in 2009 and ANSI in 1996. Related to PDS ecosystem, the Qiy foundation – based in the Netherlands – is promoting the adoption of an open standard that would facilitate access to personal data generated by third party providers. Qiy enables consent based data sharing which can also be anonymised if necessary. This proposed standard enables other people and companies to subscribe to a person's information node and given the user's consent receive updates when this information gets updated. The framework essentially provides a user centric model of managing personal information, adding consent and anonymisation layers which users control[82].

Healthcare specifically would benefit substantially from an interoperable PDS system. Key benefits of interoperability in healthcare, which are currently facilitated by expanding EHR systems and could potentially be further enabled by a widespread PDS system, include:

- Easier and faster access to patients' information;
- Better diagnosis, better quality of treatment, and better patient safety;
- Improved cost effectiveness;
- Increased consumer choice and enhanced competition.

As discussed in the President's Council report on Big Data and Privacy, "One way to enable scalable data exchange and new application development is through the adoption of standardised metadata that enables patient data to be indexed, queried, transmitted, and re-assembled for different uses." This is essentially an XML-based approach to data storage, but it should be noted that there is not yet a recognised standard for health metadata. For the big-data benefits in healthcare research and efficiency enabled by consent-based user information sharing to be possible, significant cross-compatibility and easy-access to standardised information is essential[83].

"In relation to the Directive on the application of patients' rights in cross border healthcare 2011/24/EU, eHealth has also the potential to facilitate the implementation of rights of EU citizens to be treated abroad by ensuring continuity of care along the care pathway."[84] ■

3.5 Technical Solutions to Legal Requirements

Advances that blend law and technology may also alleviate some of the legal challenges PDS providers face. For example, concepts such as 'smart contracts' arose out of cryptography circles in the late 1990s[85]. This term refers to computer programs that assist in the automation of contract enforcement and negotiation[86]. In other words, such technologies aim to create "a set of promises, specified in digital form, including protocols within which the parties perform on these promises."[87]

One salient example of these technologies is 'Link Contracts', enabled by the XDI protocol suite, and developed substantially by at least one PDS provider. Current SMEs within the PDS space are attempting to create and use such technologies to facilitate trusted, consent-based, and secure data exchange, as well as to verify identities of network members. They are key components of what these developers term 'Trust Frameworks', or legal and technical rules (potentially certified by an authoritative governmental body) that members of a network must agree to in order to operate within the system[88,89].

[82] *Interview with Qiy Foundation*, 2015.

[83] President's Council of Advisors on Science and Technology, *BIG DATA AND PRIVACY: A TECHNOLOGICAL PERSPECTIVE*, 2014.

[84] Nicole Denjoy, *eHealth Stakeholder Group report Perspectives and Recommendations on Interoperability*, 2014.

[85] Glatz, *What's a Smart Contract?*, 2014.

[86] Cassano, *What Are Smart Contracts?*, 2014.

[87] Szabo, *Smart Contracts: Building Blocks for Digital Markets*, 1996.

[88] Open Identity Exchange, *OIX Trust Frameworks*, 2015.

[89] Mydex CIC, *The Case for Personal Information Empowerment: The rise of the Personal Data Store*, 2010.

The XDI standard that has the potential to facilitate the diffusion of PDSs as well as to mitigate the security vs. convenience tradeoff through easing the user burden in consent-based downstream data processing. As discussed in Section 3.4 (Page 23) and Section 2.2.3 (Page 12), one of the technical capabilities enabled by a PDS framework is the provision of 'link contracts' – or 'sticky policies' – that are embedded with the data. This technical, automated implementation of contracts and policies ensures that the third party data-user follows the individual's consent and data handling preferences. The third party data-user physically cannot override the individual's preferences, and they can only access the data within the timeframe specified by the individual. The individual may also specify automatic blocking or deletion of the data. The PDS provider or a trusted third-party service encrypts and decrypts the data, so long as the link contract permits this action. Some of these capabilities have already been implemented by the RESPECT Network's XDI protocol, though other implementations are also possible[90]. The concept is illustrated in Figure 10 on Page 27.

3.6 Conclusion

Technological development, in terms of both standards and computing capability, is at the level where permutations of business models can emerge while satisfying legal, security, and cost hurdles for a highly scalable and pervasive PDS service. Mainstream adoption of cloud computing produces economies of scale, which decreases computational and storage cost, consequently lowering entry barriers for emerging PDS services. The flexibility of cloud-based services allows individuals and firms to experiment with various PDS implementation, uncovering new market need and establishing dominant technologies in the ecosystem[91]. Several standards already exist that promote interoperability and secure data exchange among various digital services. Examples such as oAuth and HL7 could facilitate secure information transfer in the PDS ecosystem. Additional layers of trust framework and link contracts enforcement are also technologically available such as XDI and Qiy scheme, which further facilitate secure information handling. This is an area where the EC could help facilitate greater interoperability, promoting coordination to increase harmonisation across the industry within the EU; this would be particularly useful at the level of semantic interoperability for enabling the broad social benefits of healthcare data.

The 'link-contract" technologies, provide several advantages to the PDS concept such as consent-based data management which can travel with the data, minimising user burden and ensuring that downstream processors adhere to user preferences that encourages PDS services to evolve. These privacy-enhancing technologies may also act as legal instruments (i.e. various possible implementations of link contracts or 'sticky policies'), creating a technical means to verify compliance with data handling prescriptions. These technologies are beginning to address the divide between big-data benefits and growing concerns over privacy[92].

[90] Pearson and Mont, "Sticky policies", 2011, pp. 60–68.

[91] Ries, *The Lean Startup*, 2011.

[92] Spiekermann and Novotny, "A vision for global privacy bridges", 2015, p. 181.

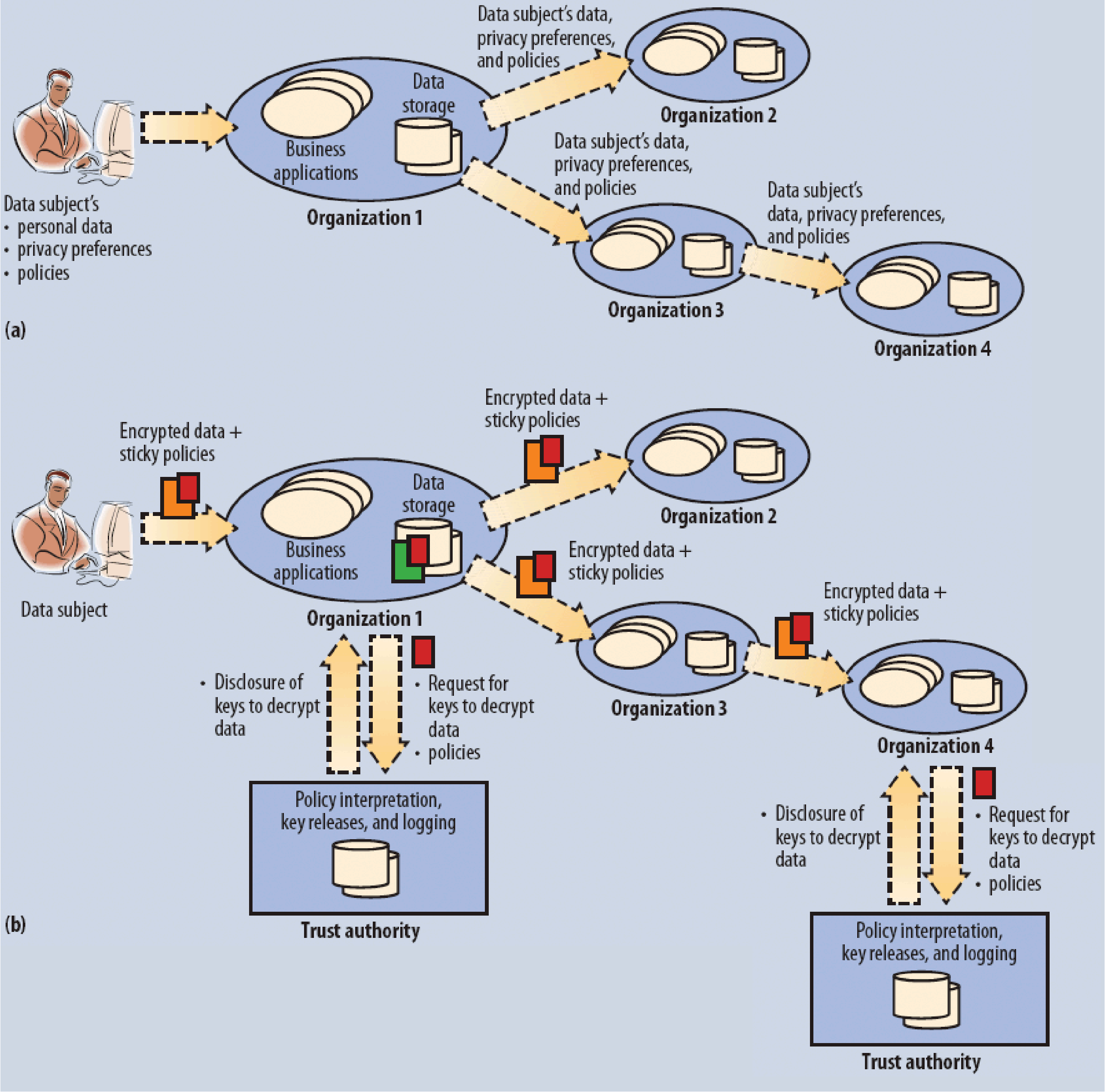

Data subject's data, privacy preferences, and policies
Data storage
Business applications
Organization 2
Data subject's data, privacy preferences, and policies
Data subject's
• personal data
• privacy preferences
• policies
Organization 1
Data subject's data, privacy preferences, and policies
Organization 3
Organization 4
(a)
Encrypted data + sticky policies
Encrypted data + sticky policies
Data storage
Organization 2
Business applications
Data subject
Encrypted data + sticky policies
Organization 1
Encrypted data + sticky policies
• Disclosure of keys to decrypt data
• Request for keys to decrypt data
• policies
Organization 3
Organization 4
Policy interpretation, key releases, and logging
Trust authority
• Disclosure of keys to decrypt data
• Request for keys to decrypt data
• policies
(b)
Policy interpretation, key releases, and logging
Trust authority

Figure 10: High-level scenario and data management diagram comparing (a) the standard approach with (b) a 'sticky policy' or 'link contract' approach. With link contracts, the data-use policies consented to and permitted by the data subject travel with the data, and only by meeting the conditions required by the policy will the requesting organisation be granted the keys to decrypt the data.

4. Economic & Business Considerations

4.1 Introduction

This section begins by discussing how much value a mainstream personal data store ecosystem might unlock for individuals, consumers and society. Then, it roughly estimates the market for personal data spaces to answer the question, "how much profit-potential is there to motivate PDS entrepreneurs to innovate in this space?" A complementary section examines the risks and benefits a mainstream PDS ecosystem poses to current market players, focusing on (1) giant data controllers and (2) SMEs.

Having explored the macroeconomic implications of PDSs, it follows naturally to explore business cases for PDSs. Beginning with a theoretical model of innovation diffusion, the report highlights the natural hurdles that block the adoption of radical new technologies. Because PDSs are network-based innovations, PDS providers face a critical mass issue, which is particularly complex to tackle when it comes to a double-sided market. After suggesting strategies to overcome this hurdle, the report turns to examples of value propositions, advertising and publicity strategies, and revenue models. The conclusion summarises numerous business models that early PDS providers are testing today.

4.2 Macroeconomic Impact of a PDS Ecosystem

> "Personal data is the new oil of the internet and the new currency of the digital world."
>
> *Maglena Kuneva (Former European Consumer Commissioner (2007-2010))*

The purpose of the following analysis is to assess the macroeconomic impact of a PDS ecosystem. It is currently impossible to measure the direct value-creation potential of PDSs because:

1. Social benefits such as 'consent' and 'control' are intangible and difficult to quantify;
2. Many of the measurable economic benefits would be secondary or tertiary effects, whereby a PDS enhances trust, subsequently enhancing the flow of personal data, making more personal data applications possible.

Rather than directly measuring the value-creation potential of PDSs, therefore, the following analysis draws on recent estimates regarding the value-creation potential of personal data applications. The value-creation potential of PDSs and of personal data applications are linked, but not one and the same. The discussion below (1) explains the Boston Consulting Group's insights into the value of personal data applications; (2) contextualises these estimates in two PDS ecosystem scenarios.

4.2.1 The Link Between Personal Data Applications and PDSs

A PDS ecosystem may stimulate personal data applications ranging from personalised products, to apps that simplify daily life, to analytical insights. As described in Section 2.2.2 (See Page 11), a PDS ecosystem could give companies that currently find data acquisition, management and compliance costs prohibitively expensive the ability to more easily and cheaply utilise consumer data. Also, richer, cleaner data sets could improve big data analytics. A useful starting point for estimating the value-creation potential of PDSs is therefore the value that personal data applications can deliver. The Boston Consulting Group conducted a detailed analysis on this topic in 2012 in the context of the EU economy[93].

[93] Boston Consulting Group, *The Value of Our Digital Identity*, 2012.

4.2.2 The Value-creation potential of personal data applications

In 2012 the Boston Consulting Group estimated how much value personal data applications might offer to eight sectors – traditional production, retail, financial services, telecommunications/media, public sector/health, social media, eCommerce, and entertainment. For each sector, they listed data applications of particular importance (for example: targeted marketing, loyalty cards) and then summed the estimated value-creation potential of all of those data applications given the sector's market size. BCG helpfully divided 'value-creation potential' into three sub-categories: consumer value, business value, and public value, defined as follows[94]:

1. Consumer value: "The value for individuals includes the consumer surplus of Internet services; lower prices (or taxes) resulting from organisations passing back efficiency gains they derived from using personal data; and time savings achieved via self-service and other digital identity applications"
2. Business value: "For private-sector companies, organisational value consists of additional revenues along with the cost savings that remain after any hand-backs to consumers"
3. Public value: "The value for governments and the public sector includes increased tax revenues and spending reductions (nearly all of the latter, however, are expected to be handed back to citizens in the form of tax reduction or other relief)"

Across all sectors, BCG estimated, personal data applications could deliver €670 billion in economic benefits to European consumers by 2020[95]. Further, personal data applications could deliver €330 billion worth of economic benefits to private and public organisations. Examples of personal data applications contributing to this value creation include:

1. Process automation: digital authentication enables self-service, for example, online credit card payments and bank balance queries;
2. Personalised products and services: observed data enables product recommendations based on browsing history; for example, some clothing companies have already started using climate data from customers' hometowns to personalise product suggestions;
3. Operational insights: richer, cleaner, larger data sets enable new insights; for example, United States insurance company Wellpoint and computer and software manufacturer IBM are working together to generate new treatment ideas from their internal data, medical research, and population health data;
4. Better focused research and development: cleaner, richer datasets reduce guesswork, allowing companies to focus their product and service development on consumer preferences;
5. Monetisation through sales to third parties: for example, a product manufacturer might want to purchase an eCommerce company's data on customer purchases.

As detailed in Table 1 (Page 30), BCG estimated that personal data applications could offer EU citizens and organisations total economic benefits of over €1 trillion annually by 2020.

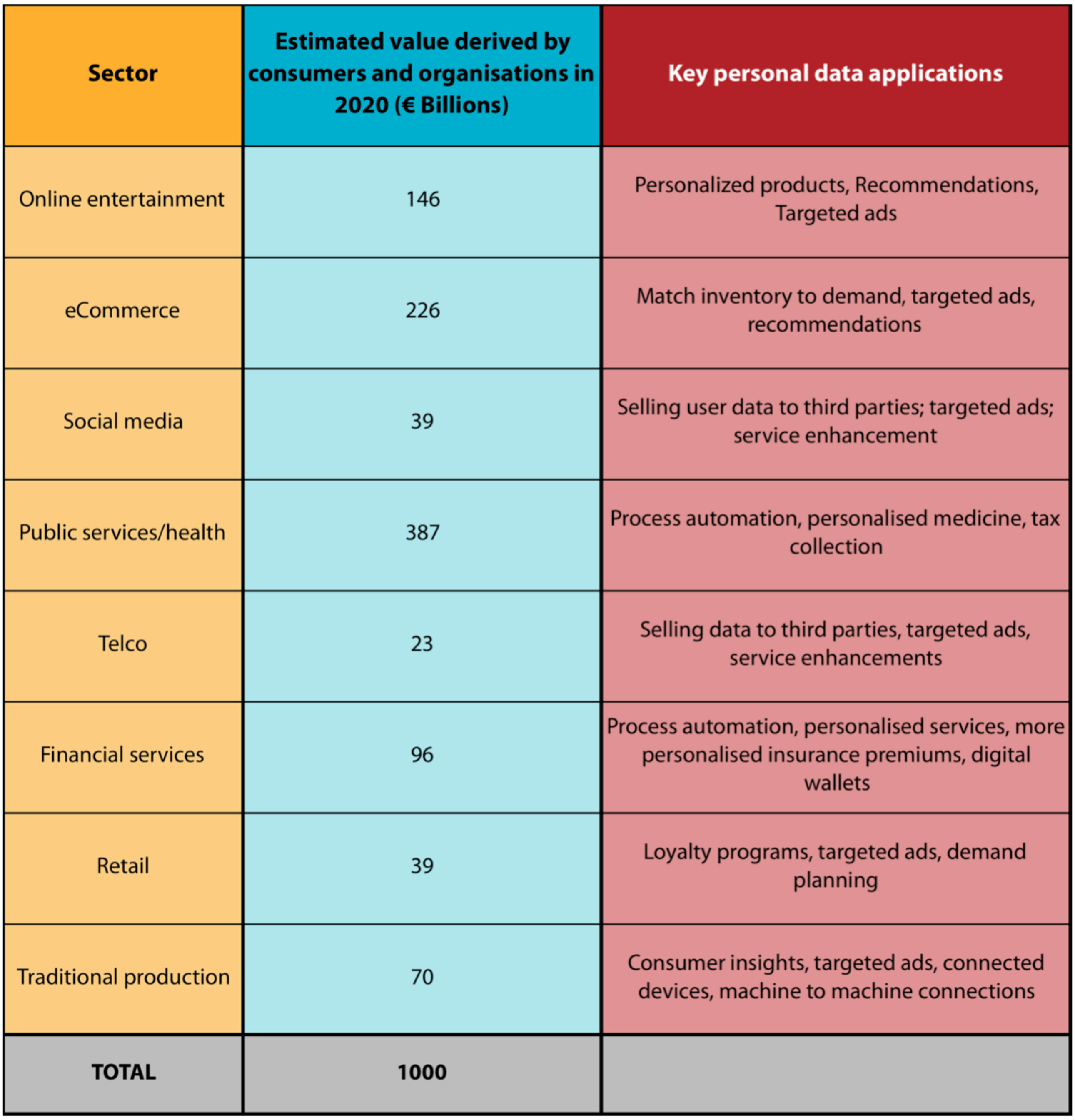
However, BCG wagers that two-thirds of the-value creation potential of personal data applications "is at risk if stakeholders fail to establish a trusted flow of data"[96].

4.2.3 Contextualising

Two scenarios are plausible when envisioning the future of a PDS ecosystem. On the one hand, when consumers can collect their personal data and choose the terms under which it is subsequently used, they may become more willing to disclose relevant, accurate information to businesses. Businesses, in turn, will gain access to richer, more accurate datasets around which to develop personal data applications. Ideally, this 'enhanced sharing' scenario will prove true (See Figure 11 on Page 31).

On the other hand, no one can claim with certainty that PDSs will enhance trust or induce users to share more information with third parties than they currently do. Instead, individuals might adopt PDSs because

[94] Boston Consulting Group, *The Value of Our Digital Identity*, 2012, p. 56.
[95] Boston Consulting Group, *The Value of Our Digital Identity*, 2012, p. 3.
[96] Boston Consulting Group, *The Value of Our Digital Identity*, 2012, p. 3.



Sector	Estimated value derived by consumers and organisations in 2020 (€ Billions)	Key personal data applications
Online entertainment	146	Personalized products, Recommendations, Targeted ads
eCommerce	226	Match inventory to demand, targeted ads, recommendations
Social media	39	Selling user data to third parties; targeted ads; service enhancement
Public services/health	387	Process automation, personalised medicine, tax collection
Telco	23	Selling data to third parties, targeted ads, service enhancements
Financial services	96	Process automation, personalised services, more personalised insurance premiums, digital wallets
Retail	39	Loyalty programs, targeted ads, demand planning
Traditional production	70	Consumer insights, targeted ads, connected devices, machine to machine connections
TOTAL	**1000**	

Table 1: Value creation: The Boston Consulting Group's estimates of personal data applications' value-creation potential in Europe (2012)

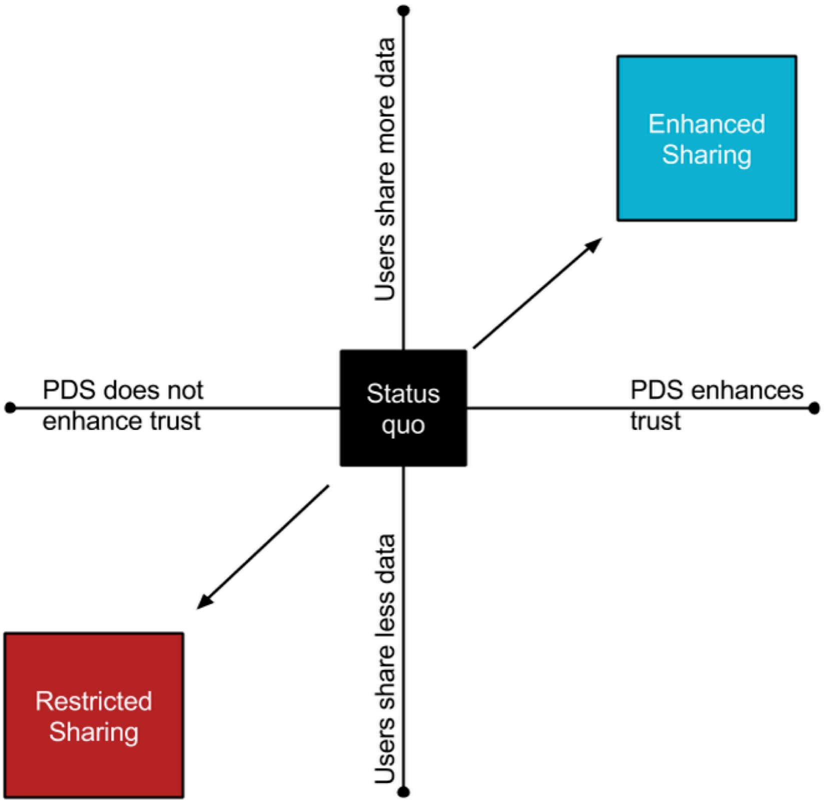


Figure 11: Possible PDS scenarios: the effects of a personal data ecosystem are uncertain and dependent on individuals' behaviour

they distrust third parties and dislike when third parties use their information. Under this scenario, 'restricted sharing' (See Figure 11 on Page 31), individuals would use the enhanced control PDSs offer to hide their data from third parties.

In order to contextualise the value of personal data applications in each scenario, it is useful to set a baseline. BCG estimates that €443 billion of personal data applications' value would be lost "if stakeholders fail to establish a trusted flow of data." Since their study does not envision a PDS ecosystem in the future, this provides a cynical baseline for comparison.

In the 'enhanced sharing' scenario, PDSs will increase the flow of personal data, enabling the development of more personal data applications. As a result, PDSs could help unlock some or all of that €443 billion currently at risk.

Alternatively, if consumers distrust data-collecting organisations and have the ability to restrict the organisations' access to their personal data – as in the 'restricted sharing' scenario – the value at risk may rise even higher than €443 billion.

4.2.4 Likelihood of scenarios

Which scenario ('enhanced data sharing' or 'restricted data sharing') comes true depends on whether individuals prioritise privacy or services. In 2014 EMC surveyed 15,000 individuals worldwide to better understand the tradeoff between privacy and convenience (See Figure 12[97] on Page 33). Results indicated that willingness to trade privacy for convenience varies across countries: India is the most receptive of the 15 nations surveyed, with 49% of respondents say they would be willing to make the trade, while Germany is the least, with only 33% reporting willingness. The EU spread itself across the rankings as follows: Italy 6th, Russia 7th, France 8th, the UK 12th, the Netherlands 13th, Germany last[98]. In addition, alleged willingness to share depends (in descending order) on whether the recipient is: a government agency, a medical institution, a financial institution, an online retailer, or a social media service. Thus, the effect PDSs will have on individuals' data sharing preferences depends on numerous factors, from the immediate context of the sharing to the broader cultural clime.

Nevertheless, both the BCG and EMC reports cited above provide evidence for optimism. The EMC Privacy Index suggests that enhancing individuals' control over their personal data may very well enhance their willingness to share such data: 84% of respondents reported that they do not like when "anyone knows anything about themselves or their habits unless they make a decision to share that information"[99]. When BCG surveyed over 3,000 Europeans in 2012, they found that privacy management tools increased consumers' willingness to share data: those individuals who were able to change privacy settings and refuse certain data uses were 52% more likely to share information than individuals who lacked such controls[100]. However, for sensitive data, like health data, willingness to share was not as correlated to the availability of control mechanisms. The incorporation of technical frameworks which act as legal tools to enable consent-based downstream data processing may also mitigate the trade-off between security and convenience (See Section 3.5 on Page 25). If they manage to enhance trust, control, and willingness to share, PDSs could decisively contribute to unlocking much of the €443 billion BCG estimates are at risk annually in the EU by 2020 with no such system in place.

[97] EMC, *EMC Privacy Index*, 2014.

[98] EMC, *EMC Privacy Index*, 2014.

[99] EMC, *EMC Privacy Index*, 2014.

[100] Boston Consulting Group, *The Value of Our Digital Identity*, 2012, p. 41.

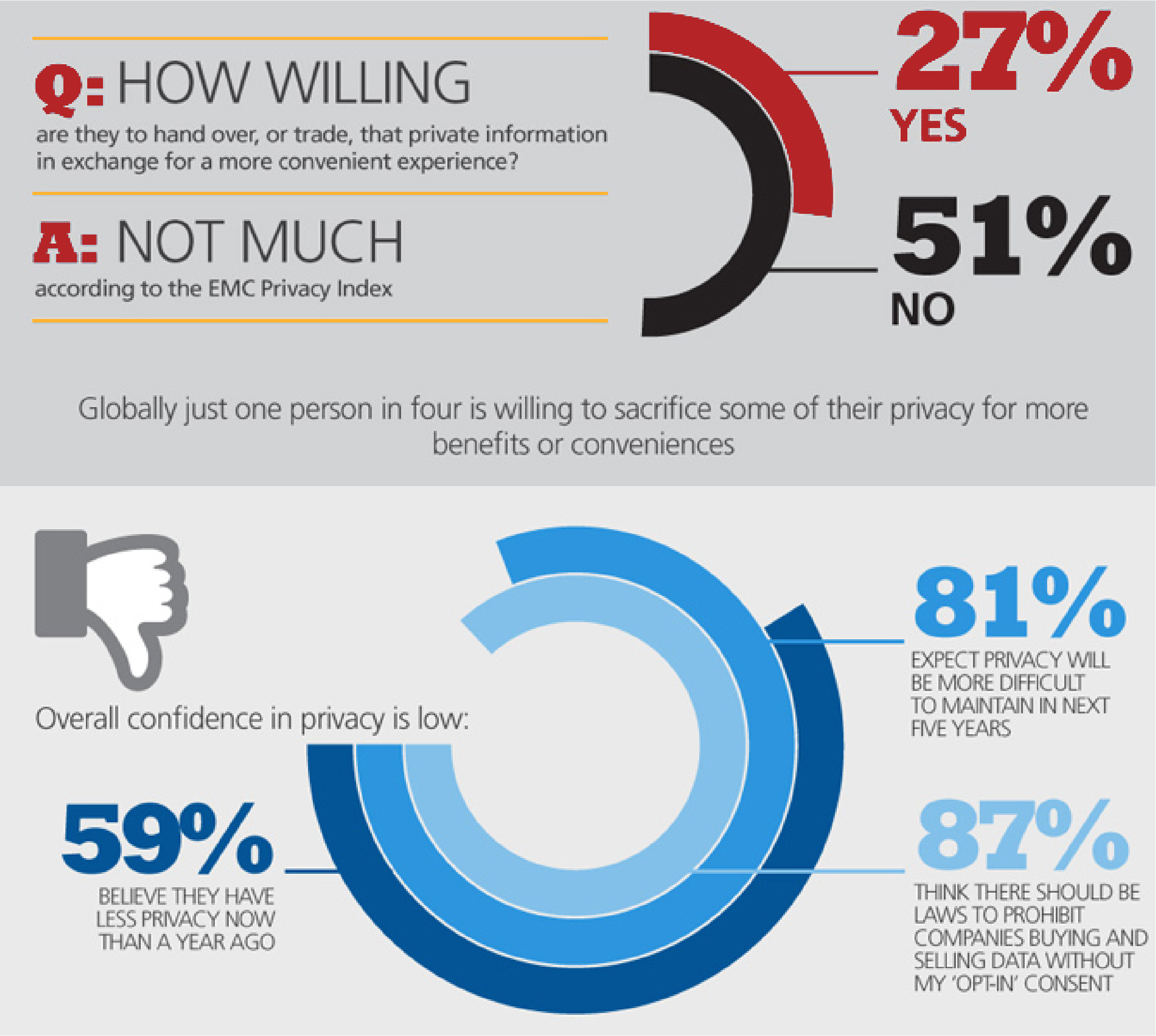


Figure 12: Confidence, privacy, and sharing: worldwide, individuals claim to be reluctant to exchange private information for convenience.

Health Case Study — Potential Macroeconomic Benefits
At the macro level, GSMA estimates that mHealth applications could save, in total, €99 billion in the EU in 2017. Of particular pertinence to the PDS concept are the savings that would arise from remote monitoring and patient data management systems. GSMA estimates that remote monitoring services could save Europe €32 million by 2017. On data management, GSMA found that doctors spend 30% of their time collecting and analysing patient data today[101]. PDS systems have the potential to reduce time spent gathering relevant patient information. Denmark, which possesses one of the most advanced e-health system within the EU, illustrates well the efficiency gains brought by eHealth: each doctor enjoys time-savings of 50 minutes on average per day and phone calls with patients have decreased by 66%[102].

PDSs improve health data sharing, which is particularly interesting in the context of chronic diseases. Due to the extension of life expectancy, the number of persons suffering from chronic diseases has increased dramatically – in France, for example, some 15 million persons suffer from chronic diseases[103]. In 2009, French public health insurance expenditures for chronic diseases amounted to €65 billion, representing 29% of total healthcare expenditures country-wide[104]. Cost savings that would arise from the roll-out of eHealth systems for only four major chronic diseases are estimated between €925 and €12,035 per year per patient[105]. This represents a minimum cost savings of €3.9 billion for the whole country. Finally, EHR rollout costs are low in comparison to potential benefit; in France, a report from La Cour des Comptes estimated this cost at roughly €1 per record[106].

4.3 The Potential Market Size for PDS Providers

As detailed above, PDSs may unlock tremendous value for Europe. How much might citizens and organisations be willing to pay for PDS services, in return? Is the market large enough to incentivise PDS providers?

Ctrl-Shift, a UK-based consultancy focused on the personal information economy, estimated the market size for personal information management systems (PIMS) in the UK in 2014[107]. According to their research, to gain "permissioned access to individuals' data and permissioned communications with customers," organisations are willing to pay on the order of £3-5 per relationship. Further, they estimate that each individual in the UK maintains between 30 and 100 relationships with banks, apps, retailers, government agencies and other organisations. Combining these two estimates with the number of adults and households in the UK, Ctrl-Shift estimates that the market for PIMS in the UK is on the order of £11.5 billion. Clarification of the estimation process is shown in Table 2 on Page 34.

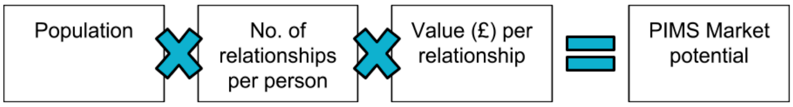
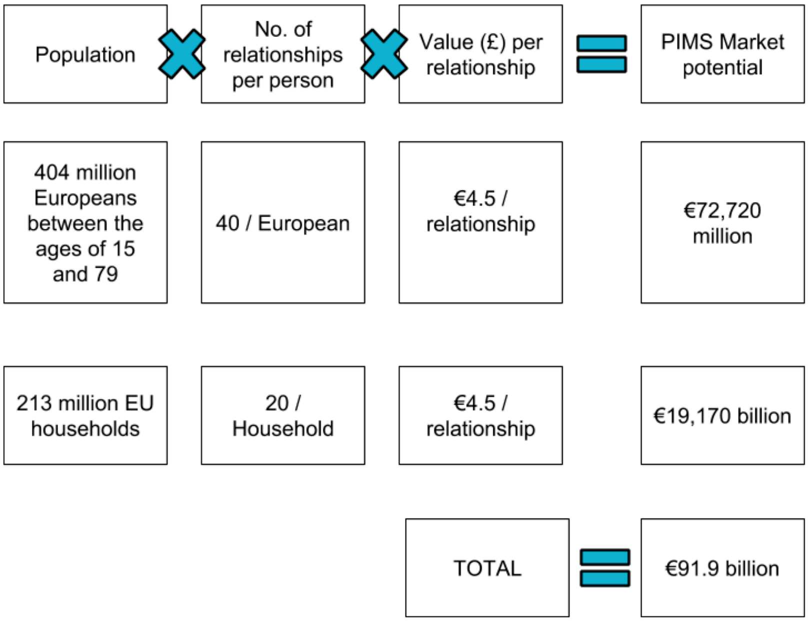


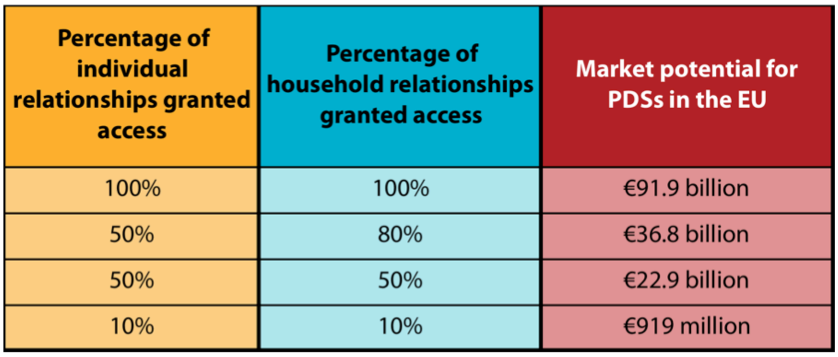
Table 2: Simplified Ctrl-Shift model for estimating the market potential of personal information management systems

[101] GSMA and PricewaterhouseCoopers, *Socio-economic impact of mHealth: An assessment report for the European Union*, 2013.
[102] ASIP, *La e-sante, secteur de croissance au service de notre systeme de sante* .
[103] ASIP, *La e-sante, secteur de croissance au service de notre systeme de sante* .
[104] l'Assurance Maladie, *Cout des ALD en 2009*, 2015.
[105] ASIP, *La e-sante, secteur de croissance au service de notre systeme de sante* .
[106] ASIP, *La e-sante, secteur de croissance au service de notre systeme de sante* .
[107] Ctrl-Shift, *Personal Information Management Systems: An analysis of an emerging market*, 2014.



Population	No. of relationships per person	Value (£) per relationship	PIMS Market potential
404 million Europeans between the ages of 15 and 79	40 / European	€4.5 / relationship	€72,720 million
213 million EU households	20 / Household	€4.5 / relationship	€19,170 billion
		TOTAL	€91.9 billion

Table 3: PDS market estimate for the European Union



Percentage of individual relationships granted access	Percentage of household relationships granted access	Market potential for PDSs in the EU
100%	100%	€91.9 billion
50%	80%	€36.8 billion
50%	50%	€22.9 billion
10%	10%	€919 million

Table 4: Value creation range: under a fee-based revenue model, the market potential for PDSs in Europe depends on how willing individuals and households are to grant sharing access to third parties.

Adapting the Ctrl-Shift methodology to the entirety of the EU provides a 'best guess' estimate of the market potential of a European-wide PDS ecosystem. No dominant business model has yet emerged amongst PDS providers, but 'relationship fees' are one method being tested today. The estimate that follows assumes all PDS providers generate revenue through relationship fees. Because willingness to pay for privacy is infrequently studied and difficult to measure[108], the estimate adopts Ctrl-Shift's £3 per relationship value. It also assumes that all EU households and all EU citizens between the ages of 15 and 79 maintain relationships with numerous organisations.

It is unlikely that individuals and households will approve PDS access for every organisation with which they interact. Table 4 (See Page 35) shows how the market potential might vary depending on individuals' and households' willingness to grant organisations access to their personal information:

As with BCG's calculation of the value-creation potential of personal data applications (See Section 4.2.2 on Page 29), the result is dependent on individuals' willingness to trust data-collecting organisations. A range of scenarios is highlighted in Table 4 (See Page 35): the most optimistic scenario of 100% willingness to share with organisations to a lower bound, pessimistic scenario of 10% willingness. Under the assumptions stated, allowing 'willingness to share' to vary, the market potential for personal data stores thus ranges from some €1 billion to €90 billion in Europe.

[108] Haddadi et al., "Personal Data", 2015.

Health Case Study — Potential Market
According to an industry report from GSMA and PwC[109], the global mHealth market will reach $23 billion USD – of which the EU will account for $6.9 billion – by 2017. Monitoring services will claim the largest market share (two-thirds), focused on chronic disease management and care for the ageing. Personal health data stores could play an integral role in enabling such services to take flight. They could also play an integral role in the improvement of information lookup systems and decision support systems, which will account for an estimated 5% of the global market in 2017[110]. ■

4.4 Risks and Benefits for Current Players

The previous sections attempt to quantify the benefits that personal data spaces offer EU organisations, consumers and PDS providers. This section discusses how an individual-centric system of data collection and control might affect today's incumbent major players and small and medium enterprises (SMEs).

As described in the introduction, technology multinationals such as Google, Amazon, Facebook and Apple are powerful players in today's personal data ecosystem. The diffusion of personal data spaces may pose risks and benefits for these companies. Today, consumers have little choice but to accept lengthy terms and conditions in exchange for online services, and most do not read the terms and conditions they accept[111]. However, when PDSs enable 'permissioned exchanges' and 'privacy-friendly' alternative services, customers may choose to opt-out of the current ecosystem and move into the privacy-friendly ecosystem. However, as mentioned in Section 4.6 (See Page 41), customers would do so only if they can access services similar to the ones they were using previously through the PDS. If the switch is feasible, customers could leverage purchasing power to ask the multinational technology giants to implement permissioned control. They could also request that the multinationals devolve their data. Or, in the extreme, they could refuse to exchange personal information for services. Internet companies could react either by abiding by the privacy terms set by the PDS, or by forcing the customer to opt-out of their 'free' services – requiring monetary payment to replace data payments. The reaction would strongly depend on the number of customers willing to move into the PDS ecosystem. Because the current business models rely heavily on selling user data to advertising agencies, losing access to large stores of personal data is a sizeable risk[112]. If individuals turn out to be unwilling to let internet companies monetise their personal data, the current paradigm under which free services are traded against freedom of use of personal data could be threatened. The risk is especially high for social media companies, as they receive the lowest trust ratings – the EMC Privacy Index[113] found that only 39% of individuals worldwide feel confidence in the ethics of social media companies.

On the other hand, the rise of personal data spaces poses potential benefits to the multinationals. Permissioned data exchanges and more flexible terms of exchange would allow them to feel new confidence in collecting, analysing and selling personal data. The legal certainty that PDSs provide could reduce compliance costs by ensuring individuals' explicit and unambiguous consent. Also, the big-data benefits of PDSs could magnify other revenue streams. A PDS ecosystem could increase the visibility of data resources available for analytics, and this could enhance demand for existing analytical consulting services. Many of the multinational technology giants have powerful analytics capabilities, in addition to their own data resources. An estimated $17 billion will be spent on big data analytics in 2015 with a 40% cumulative annual growth rate[114], making this an attractive strength on which to focus.

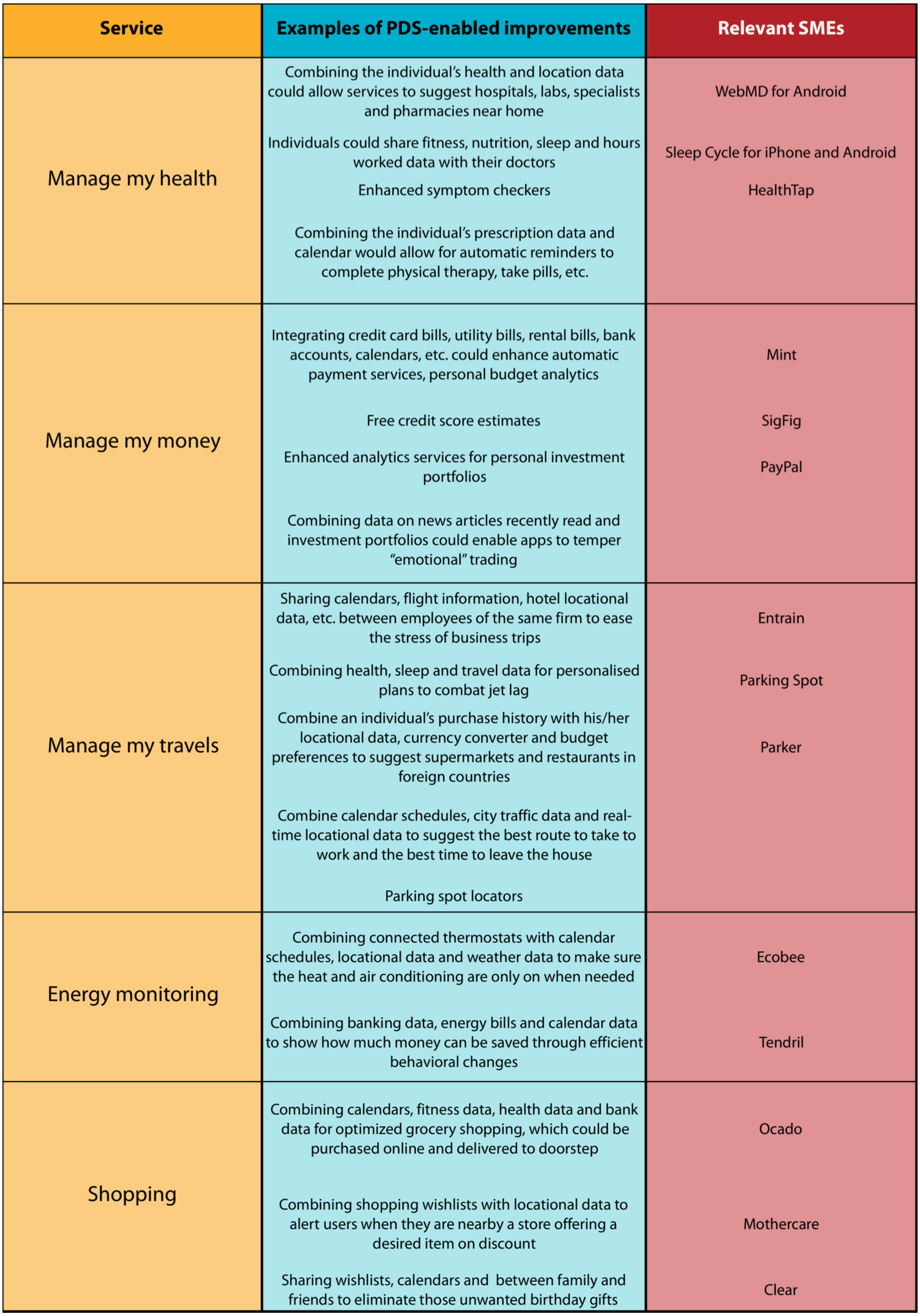
PDSs also potentially pose risks for small and medium enterprises. If PDSs were to enhance consumers' trust in the multinationals, for instance, small and medium enterprises might find it even more difficult to compete. If, for example, consumers today are hesitating to engage with multinationals because they cannot control what the multinationals do with their data, providing them with this ability may increase en-

[109] GSMA and PricewaterhouseCoopers, *Socio-economic impact of mHealth: An assessment report for the European Union*, 2013.
[110] Vishwanath et al., *Touching Lives through Mobile Health*, 2012.
[111] Forum and Group, *Rethinking Personal Data: Strengthening Trust*, 2012, p. 23.
[112] Ctrl-Shift, *Personal Information Management Systems: An analysis of an emerging market*, 2014.
[113] EMC, *EMC Privacy Index*, 2014.
[114] Boston Consulting Group, *The Value of Our Digital Identity*, 2012.

gagement with multinationals rather than SMEs. Additionally, PDS-enhanced transparency might lead to price wars that disadvantage SMEs, based on easier price, product and service comparisons[115].

The potential benefits for small and medium enterprises are manifold. With the exception of public data sets, large data sets are currently the siloed property of the multinational corporations that pay for their collection and storage. Obtaining access is expensive for SMEs. When SMEs try to collect and store their own datasets, they face high compliance and cyber-security costs. Were consumers to embrace the PDS concept, however, small and medium enterprises could query as few or as many customer PDSs as they like for accurate, rich data at a much lower cost. With personal data both more accessible and more affordable, the playing field for personalised services, demand-sensitive inventory requests, demand-driven R&D, etc. might equalise. Further, a PDS ecosystem could enhance or spur services in numerous categories, as described in Section 4.2 (See Page 28). Table 5 (Page 38) suggests some examples of healthcare, financial, travel, energy and retail sector data applications.

[115] Ctrl-Shift, *Personal Information Management Systems: An analysis of an emerging market*, 2014.



Service	Examples of PDS-enabled improvements	Relevant SMEs
Manage my health	Combining the individual's health and location data could allow services to suggest hospitals, labs, specialists and pharmacies near home Individuals could share fitness, nutrition, sleep and hours worked data with their doctors Enhanced symptom checkers Combining the individual's prescription data and calendar would allow for automatic reminders to complete physical therapy, take pills, etc.	WebMD for Android Sleep Cycle for iPhone and Android HealthTap
Manage my money	Integrating credit card bills, utility bills, rental bills, bank accounts, calendars, etc. could enhance automatic payment services, personal budget analytics Free credit score estimates Enhanced analytics services for personal investment portfolios Combining data on news articles recently read and investment portfolios could enable apps to temper "emotional" trading	Mint SigFig PayPal
Manage my travels	Sharing calendars, flight information, hotel locational data, etc. between employees of the same firm to ease the stress of business trips Combining health, sleep and travel data for personalised plans to combat jet lag Combine an individual's purchase history with his/her locational data, currency converter and budget preferences to suggest supermarkets and restaurants in foreign countries Combine calendar schedules, city traffic data and real-time locational data to suggest the best route to take to work and the best time to leave the house Parking spot locators	Entrain Parking Spot Parker
Energy monitoring	Combining connected thermostats with calendar schedules, locational data and weather data to make sure the heat and air conditioning are only on when needed Combining banking data, energy bills and calendar data to show how much money can be saved through efficient behavioral changes	Ecobee Tendril
Shopping	Combining calendars, fitness data, health data and bank data for optimized grocery shopping, which could be purchased online and delivered to doorstep Combining shopping wishlists with locational data to alert users when they are nearby a store offering a desired item on discount Sharing wishlists, calendars and between family and friends to eliminate those unwanted birthday gifts	Ocado Mothercare Clear

Table 5: Possible services enabled or enhanced by the PDS concept and current SMEs engaged in these areas

4.5 Innovation Diffusion

4.5.1 Introduction

While the PDS idea offers several advantages both at the granular individual level and at the societal level when compared to the incumbent offerings, PDS providers have thus far experienced difficulties gaining traction with their service offering. This is a common problem for new innovations; Moore[116] posits that a wide chasm separates the technology enthusiasts – who are early adopters – from the more reluctant masses who wait for overwhelming evidence that an innovation is worth adopting. Crossing Moore's chasm is one of the more difficult challenges that innovative enterprises face.

> "Getting a new idea adopted, even when it has obvious advantages, is difficult. Many innovations require a lengthy period of many years from the time when they become available to the time when they are widely adopted. Therefore, a common problem for many individuals and organisations is how to speed up the rate of diffusion of an innovation."
>
> *Everett M. Rogers*

4.5.2 Crossing the Chasm and Innovation Diffusion

Everett Rogers' seminal work Diffusion of Innovations[117] defines five variables that affect how quickly new ideas take hold: relative advantage, compatibility, complexity, trialability, and observability.

> **Relative Advantage:** Relative advantage refers to the degree to which the innovation is perceived as superior to ideas that it supersedes. The degree of relative advantage may be measured economically, in social prestige, convenience, satisfaction, fulfilment of desires, etc., but the greater the relative advantage the faster the diffusion and adoption.

What do PDSs supersede that they offer relative advantage over? They do not expand upon an already available product but rather they disrupt existing business models and paradigms for digital services, and norms surrounding user consent and control of data existing. They offer relative advantage for individuals, small and medium enterprises, and the public sector:

Relative advantages (Also see Section 2.2 beginning on Page 9 and Section 4.9 beginning on Page 48):

- Individuals would potentially experience the following, though providers must be careful to properly balance privacy/control/security with convenience to ensure the relative advantage is a net positive for individuals:
  - Enhancement of privacy.
  - Access to more tailored services.
  - Consent-based and opt-in control.
- Small and medium enterprises would enjoy:
  - Access to a larger, richer bank of data, allowing them to reap big data analytics benefits that would otherwise be beyond their capability to achieve. This allows them to improve value delivered to consumers;
  - More clear alignment with legal requirements surrounding data processing;
  - Reduced management overhead for data.
- Public sector could gain:
  - A variety of benefits arising from big data analytics in a range of sectors, such as city planning, health-care, procurement, public services;

[116] Moore, *Crossing the Chasm: Marketing and Selling Technology Products to Mainstream Customers (Capstone Trade)*, 1998.
[117] Rogers, *Diffusion of Innovations*, 2003.

  - Cost savings from the provision of more efficient and targeted services.

Compatibility: There are two components to compatibility: social and technical. In terms of user perception, it is mainly social compatibility which is important, as technical compatibility will be assumed on the part of the user and must be facilitated to the greatest extent possible by the innovator; users will generally be locked into an existing ecosystem and if this is to be usurped, an equal or superior ecosystem must be provided. Social compatibility mainly refers to the degree to which the innovation is perceived as being consistent with the existing values, past experiences, and current needs of potential adopters. This is particularly the case for social norms and values.

In the case of PDSs, social compatibility stems from:

- Alignment with the fundamental rights of European citizens enshrined in the Data Protection Directive (DPD) and the upcoming General Data Protection Regulation (GDPR): privacy is one of the fundamental rights of European citizens, for example, and PDS products could facilitate the shift towards greater user privacy and control of personal data.
- Europeans have voiced concerns regarding the use and misuse of their personal data; PDSs aim to facilitate and incentivise privacy by design.

However, risks to PDS compatibility include:

- Perceived centralisation could hamper social compatibility; even though PDSs do not necessarily compile personal data in a single repository, users might not understand the PDS architecture and worry that centralisation increases risk;
- Technical compatibility should not be taken for granted, as there are still several technical challenges around data portability, interoperability, and big data access while maintaining adequate information security (See Section 3.4 on Page 23 and Section 3.5 on Page 25).

Complexity: Complexity simply refers to the degree to which an innovation is perceived as difficult to understand and use by the user base. The greater the perceived difficulty in adopting a new innovation, the less likely it is to be adopted and the slower the diffusion.

In the case of PDSs, some of the existing solutions are in a 'beta' stage and appear to be quite complex and difficult to navigate for non-technical users. They have not been widely adopted. It will be essential to ensure a user-friendly and seamless experience to gain critical mass and broader adoption (Also see Section 2.2 on Page 9).

Trialability: Trialability refers to the degree to which an innovation may be experimented with on a limited basis. This also refers to lowering the barriers to entry. If there is a high entry cost and uncertain outcomes, it discourages adoption and diffusion. By significantly lowering entry barriers and making it easy for people to experiment, there will be faster diffusion as long as the innovation fills a need and satisfies the other categories.

In the case of PDSs:

- Providing PDS solutions which are – at least initially – free and that possess working and useful functionality is essential to allow users to try the concept without significant investment;
- Since the model represents a significant departure from existing business models, users may initially be critical of long-term viability; the minimisation of entry barriers would increase the likelihood that users will experiment with the services;
- Partnering with large incumbents to maximise initial value for early adopters would also be useful and create an access point for network spread;

- PDS providers should also endeavour to ensure that users are not 'locked in' and that they can leave whenever they wish (Cozy Cloud's slogan, for example, is "You will stay because you can leave").

Observability: Observability refers to the degree to which the results of an innovation are visible to others. The easier it is for non-adopters to see the benefits gained by adopters, the faster the diffusion of the innovation.

PDS providers might consider:

- Partnering with large visible companies with expansive networks will help facilitate early adoption, particularly if the partner is trustworthy and respected. Hospitals are a good PDS diffusion point for these reasons; telecommunications networks, government bodies, large companies such as Apple, and celebrities might also be useful for similar reasons.
- From an individual user's perspective, observability requires knowledge acquisition about the benefits and functionality of the service: in the case of PDSs, what type of data is accessed, and by whom? What do they do with the data, and what are the advantages? The answers must be clearly visible to users.
- From an enterprise's perspective, it is important that the upgrades and improved functionality offered by a PDS service – through additional data and analytics – are obvious. Ultimately, to gain business adoption, enterprises must perceive demonstrably more value from PDS services than their existing norm; from an observability perspective, this implies the necessity of transparency surrounding financial impact, and greater customer satisfaction.

4.5.3 Conclusion

In summary, it appears that PDSs have the potential to offer significant relative advantage over the existing data management paradigm and are compatible both technically and socially with existing trends. However, current complexity, observability, and trialability are low and PDS providers must ensure that these hurdles are overcome to ensure broader adoption.

4.6 Critical Mass and the Double Sided Market

When seeking to attract individuals and businesses within its ecosystem, a PDS faces a critical mass issue which hampers incentives to migrate towards this platform from the perspective of both users and online service providers:

- Businesses need a critical mass of individuals using the PDS to be convinced to request personal data through this platform. For businesses, then, 'critical mass' represents a threshold number of users that must be on the PDS platform for privacy constraints to be worth abiding by.
- So far, consent and control have been insufficient selling points to attract individuals to PDSs. For a PDS to attract individuals, the PDS must additionally integrate a variety of useful, trustworthy services; for individuals, then, 'critical mass' represents a threshold number of services that must be on the PDS platform to overcome switching costs of abandoning the individual's current habits.

This mutual baiting issue is not specific to Personal Data Spaces. It is encountered by any two-sided market, which can be defined as a market characterised by the presence of two distinct sides whose ultimate benefit stems from interacting through a common platform[118]. A personal data store, whatever the form it takes, falls into that category to the extent that it ultimately aims at bringing together individuals and online services on a single interface controlled by the user. To tackle this problem, a platform must target a group of users (individuals, businesses, or any sub-group) and figure out a way to be attractive to this particular group without necessarily benefiting from a significant traction amongst other groups of users. If the PDS succeeds, the presence of this group of users within its ecosystem should strengthen its attractiveness towards other types of stakeholders. This latter phenomenon is referred to by economists as 'network

[118] Rochet and Tirole, "Platform Competition in Two-Sided Markets", 2003, pp. 990–1029.

effects'[119].

An example put forth by Rogers which illustrates well the network effect is the fax machine[120,121]. The technology was in existence for over a century prior to its widespread usage and popularity. Fax technology is archetypal of the critical mass issue; while providing a very useful means of rapid document communication, the technology is useless if the individual or organisation with which you wish to communicate does not have a fax machine. The first adopter thus faces the paradox of adopting a theoretically useful but pragmatically useless machine, as they are the only user. The technology only becomes useful once a sufficient number of people have adopted it such that any individual or organisation can assume that another individual or organisation they wish to communicate with also likely has a fax machine - this is the critical mass point, which is essential for a self-sustaining innovation. For the fax machine, this point was not reached until 1987 (where demand began rapidly accelerating) despite technological capability in the late 1800s and a commercial product in the 1960s. The double-sided market dilemma is a central problem to overcome in networked technologies, and is discussed in more detail below.

Like the fax machine, telephones, email, and other digital technologies requiring networked interaction are relatively useless to a single adopter unless others also adopt the technology[122,123,124]; this is also true of the PDS concept but more complex because it is a double-sided market. Reaching a critical mass in the context of a double-sided market is more complex than in the case of a linear business because of network effects. A PDS solution in and of itself is not useful unless it is successfully integrated with the services generating the data of value to the user. A system for consent-based control of user data will only provide the level of control – in a pragmatic sense – that the user desires if the services which generate the data they want to control are integrated with the PDS system. Examples of such services are social networking sites, mapping systems, health databases, etc. These third party services are generating and using the data, where the PDS system itself only offers a means of management and control. To be successful as a service in itself, the PDS has to integrate with these third-party services to enable control. Such services will have little incentive to integrated with the PDS unless there is a large enough user pool from which they can generate value for their business.

Several strategies to overcome these issues are described in Table 6 (See Page 43), drawn from Moazed's 7 Strategies framework[125], that could help a PDS provider to reach the critical mass required to generate positive network externalities.

[119] Alstyne, Eisenmann, and Parker, *Strategies for Two-Sided Markets*, 2006.

[120] Rogers, *Diffusion of Innovations*, 2003.

[121] Holmlöv and Wärneryd, "Adoption and Use of Fax in Sweden", 1990.

[122] Kraut et al., "Internet Paradox: A Social Technology That Reduces Social Involvement and Psychological Well-Being?", 1998.

[123] Holmlöv and Wärneryd, "Adoption and Use of Fax in Sweden", 1990.

[124] Rogers, *Diffusion of Innovations*, 2003.

[125] Moazed, *7 Strategies for Solving the Chicken and Egg Problem as a Startup*, 2015.

Potential Strategies	Population Targeted	Description	Illustrating example	Relevance for PDS/ Example of PDS using this strategy
Building a cooperative strategy	Businesses	Bringing together actors sharing similar interests, and tapping into their pre-established customer base to attract individuals	Google created the Open Handset Alliance with mobile phones manufacturers around its open-source operating system Androïd, so as to gain traction in mobile internet (Android enjoys nowadays an 80% share in OS market)	Cozy Cloud targets big organizations facing technical or technological challenges and aims at leveraging their customers bases to attract individuals within its platform Digi.me includes its product in a "security bundle" of products sold at Fnac Partnerships with hospitals (Patients Know Best), banks (Digi.me), government agencies (Mydex)
Acting as a producer	Individuals	Starting as a traditional business offering products or services to build a customer base, and opening up the platform once a critical mass has been reached	Apple didn't open its App Store at the first place; it started as a traditional phones provider and opened up its applications platform to developers after having gained significant traction within the market	Proposing traditional services to businesses (cloud computing, developing environment, etc…) Endowing the PDS with a set of basic applications (analogous to applications pre-installed on a smartphone for instance) Respect Network currently plans on creating a messaging service and eventually building on data transfer capabilities
Creating Single- or Double-Sided Marquee Strategy	Individuals or businesses	Targeting users whose presence brings particular value to the platforms because other users will want to interact with them	Facebook also used this strategy to great effect by gating access to its network and opening up to Ivy League schools first. It then used the prestige of the Ivy League to help market to other schools.	Public procurement could trigger the takeoff of a PDS (for instance, Estonian government due to its strong commitment to online public services) Some PDS providers are going through hospitals as a trusted and respected diffusion point with broad market reach Universities could be a particularly relevant launch point, since they are microcosms of society and require access to students health, academic and personal data; students are tech savvy and embrace change; the prestige of certain establishments such as Oxbridge could also be valuable
Targeting a user group to fill both sides	Organizational level	Identifying and attracting a specific user group that goes into both categories at the same time	Etsy, platform for handmade goods, used the fact that the people most likely to buy handmade goods were the ones also selling them	Selling PDS as a way to access Big Data (analytics and efficiency) to small SMEs and hospitals (which generate a lot of data, but want to access more data within a more extended geographic scope) Municipalities - particularly smart cities - could be good candidates as well

Table 6: Strategies for overcoming the double-sided market

Table 6 (See Page 43) does not present all seven strategies of Moazed's framework, but rather focuses on the ones that are the most relevant to PDSs. Each platform-seeding strategy described has been used by emblematic, successful businesses such as Google, Facebook or Apple. In the light of these strategies, two main patterns of action, not mutually exclusive, emerge when it comes to tackling the mutual baiting issue:

1. Developing alternative value proposition that goes beyond the platform's core activity consisting in establishing links between two different populations: This can take the form of monetary subsidies or specific product features. For instance, high-value users mentioned in the third strategy could be attracted through monetary subsidies. Also, the second strategy clearly highlights the role of specific product features in order to attract a specific group of users.
2. Sequencing users. Identifying and attracting groups of users that are particularly relevant to the platform and using the presence of these users to catalyse the growth of the platform can prove to be much more efficient than seeking to attract users in an undifferentiated way. For instance, large organisations can give access to a broad consumer base, as described in the first strategy with Google.

Thus, reaching a critical mass is much more complex in the case of a double-sided market such as a PDS than in the case of a linear business. Having a carefully crafted go-to-market strategy that puts the emphasis on certain groups of users or on alternative value proposition is key to the success of a PDS.

4.7 PDS publicity and Network Strategy

The PDS ecosystem is undergoing a period of definition through business model and technological experimentation as it tries to find a market niche and define a value proposition for early adopters. Users, both enterprises and individuals, can expect rapid developments in terms of service maturity and expansion of offerings before the emergence of a dominant design[126]. This crucial period for PDS providers requires them to assert value propositions across a double sided market comprised of enterprises on one side and individual consumers on the other. In doing so, a PDS firm must consider the implications to its marketing programs and resources aimed at two very distinct audiences.

Firstly, to stimulate adoption by individual users, a campaign to educate consumers about the service, what problems it addresses, and why it is relevant now, needs to be crafted. Traditional, broad-based 'low touch, low cost' campaigns can address this need through social media, YouTube, and startup networks such as TechCrunch. Social media in this regard can play a significant role by targeting public figures to lead the campaign on product awareness and identify the value gap a service is addressing.

Health Case Study
Another marketing program that can be exploited is the the altruistic angle of PDS systems for Big Data health research. PDS providers in this area can leverage health research agencies to disseminate product information and tap their online networks about programs aimed at specific campaigns that may benefit from aggregated data sets. ■

Its important to note that while individual user-acquisition is important, PDS services to-date derive revenue from the Enterprise side of the market, hence marketing programs in the individual area need to be as lean as possible.

Secondly, to catalyse enterprise adoption, PDS providers need to craft an enterprise marketing and business development program aimed at highlighting the value a firm can derive from PDS services through business efficiency gains and potentially enabling new revenue sources, or both. B2B engagement require 'high touch' programs, because enterprises have complex and distinct needs. Such high touch engagements require direct business development or partnerships with development campaigns designed to enable, educate, customise and overcome adoption barriers for enterprise firms. These typically require more resources and longer conversion cycles where mass marketing efforts are not likely to be effective. High touch programs are specific and require firms to develop expertise and refine their value propositions over time.

[126] Utterback, *Dominant Designs and the Survival of Firms*, 1994.

4.8 Business Models

What must PDS providers do to successfully enter the market? Previous chapters addressed the social, legal, and technical concerns surrounding a PDS ecosystem. It is crucial that any PDS provider comply with Europe's data protection rules. It is advisable that PDS providers come up with a strategy that balances risk, cost and convenience. It is also advisable that they choose interoperable standards and protocols. This chapter has discussed obstacles that encumber PDSs from entering the market. Overcoming the obstacles requires:

1. Tackling the mutual-baiting issue: the PDS ecosystem is a double-sided market in which both sides require critical mass for entry; as such, the PDS provider must have a strong value proposition for both individuals and enterprises;
2. Monetising their service: how will the PDS provider generate revenue?
3. Publicising and networking: the PDS provider must educate the market, perhaps through advertising campaigns, and it must also educate its potential business partners to spur development of the platform and services operating on it.

To-date, entrepreneurs have tried numerous strategies in tackling the list above. Table 7 (Page 46) and Table 8 (Page 47) present their business models to summarise their efforts. An analysis of key trends in their value propositions, monetisation strategies and publicity efforts can be found in Section 4.9 (See Page 48).

	Mutual-Baiting Issue		**Monetisation**	**Publicity/Networking**	**Current Challenges**
Enterprise	**Value Proposition for Users**	**Value Proposition for Business**	**Revenue Streams**	**Diffusion strategy**	
A	Access to personal data tightly controlled by users Prevention of unilateral data hoarding Access to enhanced services collaboration between apps Users are not locked	Access to a much richer collection of personal data allowing services to deliver more value to consumers Value proposition further tailored to companies' needs thanks to a modular and cost-efficient architecture	B2B2C business model: companies pay to benefit from Company A Revenues model can differ across companies (e.g., revenues sharing, direct fees, etc…)	Focus on big companies to reach users' critical mass; companies will act as distribution canals 3-step go to market strategy: 1. Cutting edge tech users 2. Power users, through ISPs and banks 3. Mass market	Delivering a user-friendly service Formulating a clear commercial proposition for businesses Threat of GAFA
B	An digital scrapbook of one's social media history, with unique save and search capabilities The user is able to download all of her personal data and store as she likes — on personal devices, chosen cloud, etc. User will soon be able to interact with third parties through a permissioned exchange	Businesses benefit from richer, cleaner data sets for analysis Businesses build trust with consumers Businesses save money	Third parties who want access to users' data will pay "postal fees" for the transaction	Company B began by focusing on social media, because "my story" has more appeal to individuals than "my personal data;" now Company B is trying to integrate banking and health data into the same software Partnerships with large enterprises such as banks, hospitals and health/wellness consultants will provide access to a broad user-base	Publicity, visibility Making connections with large enterprises for potential partnerships
C	Benefits: convenience, time savings Services: personal data storage and organisation, secure data exchange with ability to grant/revoke third party access	Businesses benefit from richer, cleaner data sets for analysis Businesses build trust with their clients	Individuals get their PDS for free, the revenue comes from organisations and businesses that pay a fixed annual support fee and a variable connections fee	"Starting in a highly specific place, in a highly specific way:" partnership with the UK's identity assurance program, Gov.UK Verify Having establishing itself as a trusted government partner, Company C is working on expanding into industry, social housing, and perhaps health and other areas	Contracts take a long time to implement and activate Individuals say they care about privacy, but their actions say they care about time savings and convenience; people are signing up but not in bulk
D	Text messaging that is private, encrypted, and trustworthy Users gain privacy via encrypted data transfer Users gain choice: they choose with whom to share data and from whom to withold data; these sharing settings are easy to edit Users receive ⅓ of relationship revenue	Businesses benefit from better, richer data sets for analysis Businesses build trust with their consumers Businesses target advertisements at consumers who confirm interest in their products Businesses see cost savings	Enterprises pay a "relationship fee" to interact with an individual's data set; the resulting revenue is split evenly between data subjects, the Respect Network and the cloud service provider; somewhat analogous to credit card fees	Instead of trying to sell "secure data transfers," Company D has rebranded itself to sell a product consumers already know and love: text-based messaging. Soon it will introduce enhanced privacy, security and data transfer capabilities as a new feature of this app/network	Chicken and egg issue: individuals want apps on the network before they join the network, but developers want individuals before they bother building apps; Company D launched before there was an adequate number of apps to attract individual users Marketing towards individuals

Table 7: PDS existing businesses, their models, and their strategies

	Mutual-Baiting Issue		Monetisation	Publicity/Networking	Current Challenges
Enterprise	Value Proposition for Users	Value Proposition for Business	Revenue Streams	Diffusion strategy	
E	Access to aggregated health data in one spot Gain the ability to grant and revoke consent for third-party data usage Ability to monetise data if desired	Hospitals gain efficiency improvements through access to more relevant data. Big data research benefits. Fraud prevention.	Public funding. Access fee from hospitals. Data monetisation. Access fee from researchers and third-party companies. Cost-saving revenue sharing	Marketing through hospitals and also directly to consumers. Diffusion through academic contacts.	Early stage funding and building user base.
F	Integration of health data into a central location Consent based integration of third party apps More customised and tailored health apps and services Control of healthcare data	Access to standardised platform for health data integration With user consent, access to a broader range of data for more tailored services Enhanced user trust through consent based app control	Company F sells hardware, and continually expands free offerings to maintain hardware attractiveness in a competitive marketplace Portion of revenue from software sales on internal store	Extremely large user-base to access with software preloaded on hardware, and added with latest software update	Building up a set of core health applications that integrate with the service Ensuring that users trust the service and understand that their data is not monetised or used for targeted advertising
G	The individual obtains faster care and greater knowledge of her health situation The individual becomes more mobile between healthcare providers	The medical provider is able to see more patients per day, resulting in workflow improvements and increased revenue The medical provider cuts administrative costs, data processing costs, and repeat testing costs	The hospital, GP, or other medical provider pays for the software as a service	Company G first partnered with hospitals in the UK, thus reaching individuals through their medical care providers It has since expanded into 8 countries and into new sectors, including charities, prisons, researchers and pharmaceutical companies	The heterogeneity of health data processing requirements in different countries: for instance, some countries require physical storage within their own borders Lack of standards and interoperability between health IT systems
H	Internet and cloud-based health services; the ability to contribute home-collected data, messages, photos, etc. to one's own health record; analytics; permissioned sharing	Today, it is very time-intensive and expensive for organisations that deal with private medical data to build their own, compliant online or cloud-based services; Company H offers them the ability to get up-and-running in just 3 days; businesses choose where they want their data stored	Businesses pay a licensing fee to use Company H's services; additional revenue agreements vary depending on the particular client's business model	Sell first to businesses that handle health data, because health data requires the highest levels of protection, privacy and consent; then expand into other sectors, as Company H was designed to be useful for any type of data	Building competences in more legal and technical standards and regulations Strategic investment fundraising in Europe to secure growth and business development
I	Control of data Portability of health data	Insurers and health providers: cut down on the silo of records and increased operational efficiency Better provision of care - better data = more comprehensive care Later Phase: researchers and service providers paying for access to data	Now: hospitals and and insurers paying for the services as an access fee Later phases: value exchange network where everyone pays to be members of the system	Exposure of the PDS concept in stages; currently just EHCR offering but will begin to offer new services and features, expanding network	Differing health systems/requirements/regulation in member states Building up the consumer base

Table 8: PDS existing businesses, their models, and their strategies, specific to the health industry

4.9 Discussion of Business Models in Practice

As Table 7 (Page 46) and Table 8 (Page 47) demonstrate, there is not yet a dominant strategy for tackling the mutual baiting issue, for monetising the product, or for publicising and networking. Each SME has developed a unique approach, and future SMEs will likely innovate further. Nevertheless, as this section explores, some trends are emerging.

4.9.1 PDS Value Propositions

Every PDS provider needs two value propositions: a business to consumer (B2C) proposition, and a business to business (B2B) proposition. This is because the PDS ecosystem is double-sided, like other platform businesses such as Internet Providers, e-Commerce and advertising. Amongst PDS providers, the following value proposition trends have emerged:

B2C Value Propositions

Every PDS provider's B2C proposition features the following two selling points: first, convenience arising from clustering, access and control of personal data in one logical repository; and second, security and control of personal data.

- **Convenience:** Personal data aggregation can provide efficiency gains to consumers, reducing repetitive information-entry by providing a single sign-on similar to Google or LinkedIn sign-on services. This general feature is observed across numerous PDS-like startups that were interviewed for the project, and specific deployment in eHR demonstrate this compelling value to patients (See, for example, Section 4.9.1, beginning on Page 48).
- **Control:** Secondly, a PDS improves security and control over personal data that is currently dispersed amongst myriad organisations. The PDS concept can provide a single interface and control features for granting and revoking access to personal data. At the moment this feature set is still evolving among the startups that were interviewed.

Some PDS providers, however, go beyond the primary purpose of a PDS – i.e. enhancing organisation and control – and try to appeal to consumers through ancillary services. For example, Digi.me and Respect Network have both found that 'personal data management' sounds more like a chore than a selling point to the average consumer. Though their services are based on organisation and control, they have chosen to emphasise social networking, private text messaging, private photo sharing and other, more social features as the value proposition for consumers. Later, they will expose users to the consent and control benefits beyond social networking. In some sense, all of the mHealth companies have chosen this tactic, too. Being able to message a doctor, to receive faster care, to access remote healthcare advice, and enjoy personalised analytics are propositions that sound more appealing to many individuals than 'organised, accessible health records.'

Additionally, some PDS providers (such as Cozy Cloud) include in their B2C value proposition the access for users to more targeted and personalised applications and services. By enabling users to keep the most updated profile with high quality information, PDS providers set the ground for these enhanced applications. The possibility to increase the value delivered to consumers through enhanced applications and services is also part of the core value proposition to businesses.

Lastly, an alternative view on the PDS value proposition is to enable altruistic intentions. Analogous to giving blood, personal health data when aggregated with other data sets becomes a rich source of insights for health research. If the PDS concept can demonstrate that appropriate security regimes are in place to protect users while allowing health data exchange and aggregation for research, the value proposition could shift to 'doing good' by catalysing trial and adoption for this particular purpose.

B2B Value Propositions

Similarly, there are broad trends amongst B2B value propositions. These are mainly: the access to richer and cleaner data sets, trust, and legal certainty.

- Firstly, access to richer and cleaner data sets offers efficiency gains and the means to provide more tailored services. This deviates from the current practise of 'inferring' or profiling data which evolved from stitching disjointed information to form a coherent personal profile which data monetisers currently practise. Data accuracy through PDS potentially saves organisations' time and resources dedicated to profiling and instead allows them to better focus on improving services which are relevant to individuals.
- Secondly, firms currently opt-out of using personal information when they lack legal certainty on applicable use. The PDS concepts reviewed have evolving features that address the consent issue Enhanced legal certainty offers value by increasing a business's ability to run analytics. unlocking the potential for firms to process personal information and derive value from profiling and big data analytics.
- Thirdly, a PDS offers value by reinforcing a trustworthy relationship between digital companies and their customers. Trust would mainly arise from the fact that individuals would feel more confident about companies using their personal data in explicit, previously agreed upon ways.

Less common value propositions include: PDSs can enable big data analytics because they gather extensive data sets from a wide range of individuals. If data are properly anonymised and users consent to the use of their data for analytics, organisations such as health research centres or SMEs that don't have the capabilities to collect sizeable data sets could hugely benefit from this. The midata.coop model notably envisions including big data as part of its value proposition to businesses and organisations (with consent). Also, there is a growing impetus for PDS startups to cultivate a user base and leverage on network effects to draw applications and users to the platform. Linking to a PDS network therefore offers a business more extensive customer access to that whole marketplace and user-base. This is in particular part of Cozy Cloud's value proposition.

Health Case Study

Value Propositions At the patient level, mHealth PDSs have the potential to improve quality of life by reducing hours spent in the hospital and improving self-care. Luton and Dunstable Hospital documented the benefits by running a pilot program for inflammatory bowel disease (IBD) patients. Each patient gained access to an advanced mHealth personal data store – an online patient portal – offered by UK-based Patients Know Best (PKB). In addition to organisation, worldwide access, and patient-centric control, the portals offered patients a 'symptomatic assessment' feature specific to IBD. Patients could thus log onto their portals at home, rank their symptoms from none to mild to moderate to severe, and receive instant advice suggesting whether a doctor's visit was crucial or not. Further, mobile phone apps allowed patients to upload data from connected devices in their homes, such as scales and glucose monitors. A direct alert system connected the patient at home to the hospital's IBD team.

All parties benefited from health records that were accessible and updatable by both medical care professionals and patients. Luton and Dunstable Hospital found that the remote care services enabled by PKB's patient portals both limited the number of necessary doctors visits and made the necessary trips more efficient. During the trial period, the hospital saved approximately 800 outpatient appointments, an estimated 80-200 colonoscopies and unmeasurable hospital admissions and opportunistic infections, resulting in over £226,000 in savings for a test group of just 520 patients. Perhaps most importantly, patients reported greater satisfaction with their care[127]. ■

[127] Johnson, Lithgo, and Price, "UK'S first Internet based Remote Management System for Managing Stable IBD", 2013.

4.9.2 PDS Monetisation Strategies

Monetisation strategy is crucial for a successful and sustainable business model.Similar to the value proposition discussion, a PDS monetisation strategy must address both B2B and B2C sides of the market. Firms ideally should be able to capture commercial value from both sides when their services mature and become valuable enough to charge both sides of the market; however that is not currently the case with PDS-like startups. Today, most monetisation strategies remain skewed towards the B2B side of the market. Understandably, the monetisation of PDS services is largely at infancy, and firms are experimenting on various models that would create platforms and attract a sufficient user base. After reaching critical mass, they can focus on profit maximisation and broadening of the user base to mass market.

B2C Monetisation Strategy

At the moment, all SMEs offer their PDS consumers free subscription, and Respect Network and midata.coop even share potential profits from third party personal data use with individuals. Foreseeably, PDS services might exploit freemium (free for basic use, with a fee charged for a premium product with enhanced features) revenue streams from individual users once the B2B ecosystem and application matures, or when user lock in becomes sufficient such that users have predisposed behaviour of using PDS systems for their online transactions. This strategy has been employed by LinkedIn, Dropbox, and Angry Birds as examples, and while the majority of the platform users don't pay for the service, a small proportion do pay a premium sufficient to sustain the business. Digi.me has already employed this tactic. Possible incremental revenue streams from the consumer side may include consent management, online footprint tracker, and secure data storage.

In general, existing PDS-like startups today do not charge users for joining the platform and have limited B2C commercial strategies. However, it is hypothesised that PDS ecosystems and firms will undergo a period of monetisation experiments that will mature in parallel with the emergence of dominant designs or standards.

B2B Monetisation Strategy

Six out of nine SMEs interviewed for the project use a fixed enterprise subscription fee as a source of revenue. Subscription fees are levied in return for operational efficiency gains, in the case of eHR systems, and in return for access to customer profiles, in the general case. Operational efficiency translates into cost savings, justifying the enterprise subscription fees charged by the startups.

Also, four SMEs use variable transaction fees as a source of revenue. Transaction fees follow a pay-per-query structure, so they are levied based on data usage by third parties, who derive value from using the individual profiles for research or insight gathering.

Currently, the revenue generated by PDS-like startups comes mainly from businesses, not individuals, suggesting that enterprises perceive the greatest value from PDS services. Individual users, meanwhile, either expect the services to be provided by an intermediary (for example, their hospital), or have yet to be convinced that consent and control are worth paying for. Individuals' unwillingness to pay for PDS services may be attributed to the abundance of free online services, which forms the de facto model to-date – and thus their only comparison. In the foreseeable future, PDS-like startups will continue to rely on B2B revenue streams to sustain their business until consumer's evolve to see the value from their offering. This necessitates an effective marketing and education strategy.

4.9.3 PDS Publicity and Networking strategies

B2C Publicity and Networking strategies

Educating the consumer about the PDS concept is essential for reaching a critical mass of users. However, efforts should be as lean as possible, saving money and time for B2B business development.

All of the companies interviewed for this project use their websites to educate individual consumers. Designated pages called 'personal', 'for patients,' 'for individuals,' and so on, feature graphics, text and videos demonstrating the company's value proposition. Digi.me, and Mydex, in particular, have invested in embedded video clips that explain the PDS concept. Digi.me 'brings the concept to life' in an emotional advertisement that emphasises the scrapbook-like nature of one's life story, as told in photos, emails, tweets and Facebook posts. Mydex, on the other hand, focuses on convenience and time savings, emphasising the ease and control that their PDS offers. Company I attempts to inform consumers of the vast quantities of personal data they produce and disseminate through visual cues, likening each bit of data to a grain of wheat. It emphasises the PDS as a way to ethically and efficiently manage this precious resource. The downside of webpage materials is that individuals must seek or stumble upon the websites in order to find the informational videos.

In addition to posting educational material on their own websites, many of the companies also post their materials on existing networks, such as YouTube and LinkedIn. Some, such as Mydex, Respect Network, and midata.coop, have published in the academic literature to reach the research community. The health-specific companies generally do not target individuals directly, but rather rely on medical institutions such as hospitals and GPs to recruit their existing patients onto the platform. The exception is Apple HealthKit, which already has a large network of users and thus the luxury of directly introducing its service to millions of individuals.

B2B Networking and Publicity Strategies

Business development is crucial, since the majority of PDS companies interviewed generate revenue through B2B relationships.

Furthermore, enterprise customers offer PDSs their user-base. Nearly all companies interviewed therefore view business development as part of their diffusion strategy. Cozy Cloud has focused on partnerships with large corporations so as to access these corporations' user-base. Similarly, Digi.me is excited about its contract with an electronics company, because its services will be rolled out to all customers who purchase a particular 'security pack.'

Another strategy is to begin the business development process by focusing on a niche context. The most obvious examples are the health-related PDSs, which are beginning by focusing on hospitals, GPs and other medical institutions. Already, Patients Know Best has expanded to neighbouring organisations, such as health-focused charities and prisons. Pryv and midata.coop hope eventually to expand into all data types and have chosen only to begin in health data. Synergetics is focusing efforts on a health-oriented PDS, but is also expending resources in creating a retail-oriented PDS at this stage.

Mydex chose to begin with government partnerships, and is now using its success as a proof-of-concept to negotiate contracts with industry.

4.10 Conclusion

The emergence of a PDS ecosystem could unlock the economic potential represented by personal data applications. In an ideal scenario, individuals controlling their personal data through their PDS would feel more confident about granting access to these data to digital services, which would accept in return to abide by individuals' own privacy terms, because they could gain access to richer and cleaner data sets. Personal data would then fuel development of new services and applications that would generate surpluses for both consumers and organisations.

However, the occurrence of such a scenario is dependent on two main factors: first, for individuals, the translation of control over personal data into willingness to share that data; second, the capacity of PDS startups to overcome the main challenges highlighted above by coming up with a sound business model. Regarding the first point, preliminary findings drawn from various studies make the case for optimism, although there is a clear gap in the evidence required to provide a complete answer to that question. Regarding the second point, of major importance will be the strategy to overcome the mutual baiting issue and thus reach critical mass.

Part 3

5. Summary & Recommendations

5.1 Introduction

The personal data store concept is still in its adolescence. Entrepreneurs are working diligently to develop services that give individuals greater privacy, security, control and convenience than they enjoy in the current data ecosystem.

Equally important is ensuring that the product is consistent with society's values, interoperable with complimentary products, perceived as easy-to-use, and widely visible. While there are numerous individual, social, and economic benefits perceived in greater adoption and expansion of the PDS concept as highlighted throughout this report, there are several challenges which have been highlighted by the SMEs interviewed,through business model analysis, theoretical frameworks, and literature reviews. The EC can help address some of these challenges, as this section details.

5.2 Social

- Educate and engage consumers
  - The EC can facilitate visibility of the PDS idea, its benefits, and advantages over the current data norm through pamphlet publications, website descriptions and other marketing materials
  - The EC can emphasise the altruistic nature of PDS adoption (analogous to blood donation) to facilitate faster adoption
- Conduct additional research
  - The link between stated consumer preferences and behaviour in the marketplace is still unclear
  - The net impact of PDS on DSM engagement and economic growth is uncertain
  - The balance between security, cost, and convenience
  - Preferences for user data storage are unexplored

It is probable that the initial shift to a PDS ecosystem will begin with the most technologically savvy and educated consumer-base, and the wider population will be more skeptical of the services. A possible avenue to facilitate more rapid adoption and thus enable the growth of this ecosystem is consumer education. The education can be considered from a marketing perspective, and focus on many different areas of the PDS concept such as: the potential use and misuse of personal data and how PDS shift the balance of control back to the user, the myriad benefits of PDS for personalised services and centralised management, a further illumination of the inherent digital rights of European citizens, etc. Existing initiatives such as those under Action 61 of the Digital Agenda (aimed to 'educate consumers on the new media') could be used for this aim.

A further avenue of education may focus more directly on the altruistic benefits of the PDS concept, analogous to blood donation campaigns. The PDS concept would enable myriad benefits at the social level, particularly in research relating to rare diseases, and tapping into the natural altruistic tendency of people may help promote the PDS concept as not only a smart personal choice, but a smart social choice and frame it almost in the sense of an obligation.

Also, additional research is necessary. Based on currently available data, there is no clear link between stated consumer preferences and attitudes about privacy and data protection and their actual behaviour in the marketplace. Additional data on this particular point could enable a much stronger argument to be made which would link PDS usage with greater engagement with the DSM and long-term growth of the digital ecosystem; this would also enhance the general job and wealth-creating effect of fostering a new product sector. The EU is currently supporting research in the arena of online behaviour, but it would better serve adoption of services if links between attitudes and actions were more fully explored. For example, Eurostat is currently conducting a survey on ICT attitudes and usage within households and by individuals, however the data it is collecting about privacy only reflects high level management strategies.

Other important areas of further social research include determining the appropriate balance between privacy, control, and convenience (these tradeoffs may be mitigated to some degree by new technologies such as link contracts), as well as attitudes towards various technical details of PDS implementation such as data storage architectures (local vs. cloud) and the impact this may have on user trust and long-term service usage as well as the social benefits such as research access. For example, such research might take the form of ethnographic observation of users in a prototype PDS environment[128].

5.3 Legal

- Continued harmonisation of regulatory regimes
- Alleviating compliance burdens/issues of SMEs via education and consultation measures

The legal barriers to PDS dispersion stem from two main, related problems: first, the differences between data protection regimes, and second, the ensuing issues for providers in navigating these differences. On this first point, the EU has and continues to devote substantial effort at harmonising these regimes through continued negotiation and eventual implementation of the GDPR. Thus, barriers such as disparate data localisation laws will no longer be an issue in the near future. But the version of the GDPR currently under debate could be further improved. For example, from the perspective of PDS providers and individuals alike, including provisions for machine readability of personal data in regard to the right to data portability would not only increase interoperability between providers but more easily allow individuals the ability to exercise that right. This suggestion has already been made by various industry players.

But on this second point, for providers currently developing PDS systems and also those who will be navigating a more unified regulatory environment in the future, compliance can still be a substantial burden. For SMEs in particular, the EC could facilitate development of compliant, attractive PDS services by providing and publicising various educational resources. Potential measures might include:

- Further utilising the network of Member State Data Protection Agencies as educational and guidance centres; measures might include Member State-wide encouragement of dedication of resources to specialised 'Advisory Visits' similar to those conducted by the UK's ICO.
- Development of a point of contact that could specifically address industry queries about data protection or assist SMEs in navigating the various disparate resources for such issues that are provided across different EC departments - from DG Grow to the Cloud Computing unit in DG Connect.
- Embed resources (e.g., legal consultations) within existing networks such as the Enterprise Europe Network. Such networks, already styled as one-stop-shop hubs for digital entrepreneurs, could serve multiple purposes - education in particular compliance points but also facilitating general rights-protecting innovation via increased rhetoric and discussion.

In addition to providing resources such as the above, the EC would additionally need to widely disseminate information about these resources. This could be accomplished via identification of the venues and tight knit communities within which these entrepreneurs operate; conferences and panels on relevant topics directed at SMEs; general public announcements and encouraging the media to report on or profile these resources

5.4 Technical

- Facilitate platform interoperability through the discussion and promotion of industry standards
- Host or assist with the creation of PDS-specific industry conferences and events where standards and interoperability can be further promoted
- Act as the hub for platform and ecosystem discussions to reduce information asymmetry and coordination problems
- Engage the industry to push for standardised terminology, concept and attributes of PDSs

[128] Haddadi et al., "Personal Data", 2015.

The EC should work with various standard-setting bodies to continue the dialogue on emerging interoperability and standards for PDS systems and the adjacent technologies that would support the PDS ecosystem. These PDS enabling standards will form the backbone of the ecosystem and would facilitate interoperability among emerging and existing providers of digital services. These include the likes of Facebook, LinkedIn, Amazon, Google on one end of the spectrum and the various SMEs and PDS startups on the other. Interoperability and standards are the common technology thread across providers that can facilitate free movement of data towards smaller PDS providers based on service merits instead of status quo data silos.

However, in emerging industries information asymmetry and coordination problems are difficult to overcome, and the EC could act as a central information point to mitigate the concern. Additionally, the EC as a repository of domain knowledge and expertise can act as a facilitator - promoting diffusion of technologies and ideas between platforms such as Cloud, IoT, Telco and the healthcare space. Information asymmetry hinders the natural flow of services creation across these spaces and the EC is well positioned to orchestrate interactions, raise awareness of specific issues and engage the large incumbent firms to interact with the rest of the emerging ecosystem.

The EC can also spearhead information campaigns to raise the awareness on the PDS concept across technology ecosystems in Europe. These campaigns should be aimed at defining the PDS concept based on attributes and benefits of ideal technical standards since the EC has a function of conceptual promotion rather than the picking of specific standards. Given the infancy of the concept, permutations of technical and service implementation should be encouraged as well, as this expansion will validate what the market needs and highlight the value as a service while propelling dominant systems into mainstream markets.

In a more creative approach, the Commission could consider host a 'hackathon', also known as a 'codefest', or a multi-day event that brings together computer programmers and software developers to tackle a particular technical challenge. The concept is widely known amongst venture capitalists and university students, who value the friendly competition it engenders. A Commission-hosted, PDS-themed hackathon could serve as both a networking event and a problem-solving session.

5.5 Economic & Business

- Help PDS providers reach a broad user-base, through:
- Public procurement programs
- Initiating dialogues with Telecoms
- Following Apple's HealthKit
- Connect PDS providers to other personal data stakeholders through conferences and networking events
- Connect PDS providers with each other in order to foster the exchange of ideas; of particular interest is the critical mass issue in the context of a double-sided market
- Make funding sources widely visible and simple to understand

Innovations need visibility to gain traction. One way in which the European Commission could enhance the visibility of the PDS system is by encouraging Member States to consider public sector procurement of PDS services. Many public organisations, from hospitals to identity card issuers, could benefit from PDS services; their large citizen networks would mitigate the PDS providers' double-sided market dilemma, in exchange.

Like Member States, telecom operators could play a major role in catalysing a PDS ecosystem, to the extent that they benefit from several key advantages that would make them particularly relevant stakeholders in the context of such an ecosystem:

- Telecom operators have a sizeable customers base; thus, partnering with a telecom company would be a way for a PDS provider to reach a critical mass of individuals (e.g. Cozy Cloud).
- Telecom operators process significant amounts of personal data, but data processing occurs essentially in the context of services delivered to their customers. Most telecom operators don't monetise

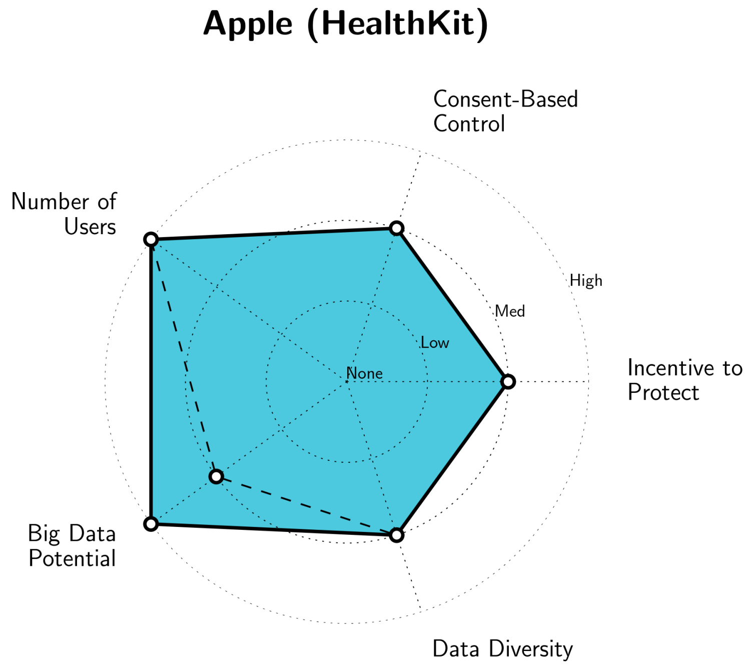


Figure 13: Apple's HealthKit could provide large social benefits if implemented with concern for privacy, security and legal compliance.

personal data by selling them to third parties[129]; thus, embracing a PDS model wouldn't generate potential conflict with their business model, unlike some major internet players such as Google or Facebook.

- Individuals trust telecom operators more than other stakeholders such as social networks with regards to their personal data : a survey recently conducted in France by CSA in 2014 revealed that 69% of French people distrust social networks, whereas this figure falls down to 33% when it comes to telecom operators[130]. Thus, the presence of a telecom operator within a PDS ecosystem could alleviate users' privacy concerns and incentivise them to transfer their personal data within this ecosystem.
- Many telecom operators have diversified their offering into digital services such as cloud computing; thus telecom operators have the capabilities required to roll-out a PDS ecosystem. In the context of eHealth, some telecom operators have positioned themselves in personal data management by offering IT solutions to hospitals that help them to manage health data flows: for instance, french telecom operator Orange provides hospitals with an IaaS (Infrastructure as a Service) solution securing the storage and the flows of patients' health data.

Thus, the European Commission could encourage PDS providers to develop strategic partnerships with telecom operators, in the form of procurement or provision.

Like telecoms, Apple has a large user-base. It also has a large developer community, and the combination, through network effects, may overcome the double-sided market dilemma discussed in this report. Apple is in the late stages of implementing a health PDS, Apple HealthKit. As the radial Figure 13 (Page 57) demonstrates, the product offers high potential for big data analytics with social benefits. Because Apple's primary business model does not include data monetisation, the company is perhaps better-placed than other technology giants to introduce the market to a health-focused, consent-based PDS service. The Commission might follow their progress.

The European Commission can also add momentum to the PDS concept by hosting conferences on the topic. Introducing PDS entrepreneurs to other data stakeholders – for instance, data protection advisors from the EU Member States, chief information officers of hospitals and public authorities, investors, university students, and telecom representatives – would both spread the word and generate connections.

[129] Vodafone, *Rethinking Personal Data*, 2011.

[130] CSA, *Les Français et la protection des données personnelles*, 2014.

Means aside, introducing entrepreneurs to one another and to other data stakeholders is important. As Chell and Baines found in their research on entrepreneurship, bringing together people who work on similar problems, but are not well acquainted with each other, has huge benefits: "The strength of weak ties is that they enable the individual to reach actively and purposively outside his or her immediate close social circle and to draw upon information, advice and assistance from a large, diverse pool"[131] (pp.196). As developed in this report, a major issue encountered by any PDS entrepreneur is the critical mass issue in the context of a double-sided market; thus, bringing entrepreneurs together would foster the exchange of most relevant strategies to overcome this issue. In short, the Commission should do its best to foster natural networking amongst PDS-interested stakeholders.

Lastly, all entrepreneurs face fundraising obstacles. Firstly, the EU should make sure that its many resources, such as the Horizon 2020 program, are widely visible. Secondly, the EU should continue to simplify and streamline access to those resources. Numerous SMEs interviewed for this project have found the Horizon 2020 program overly burdensome, and the European Court of Auditors' work recognised that those seeking funds are "still face[ing] too much red tape"[132]. Given that over 50% of early-stage funding in Europe comes from the public sector, grant applications must be clear and manageable.

5.6 Summary of Recommendations

- Educate and engage consumers
  - The EC can facilitate visibility of the PDS idea, its benefits, and advantages over the current data norm through pamphlet publications, website descriptions and other marketing materials
  - The EC can emphasise the altruistic nature of PDS adoption (analogous to blood donation) to facilitate faster adoption
- Conduct additional research
  - The link between stated consumer preferences and behaviour in the marketplace is still unclear
  - The net impact of PDS on DSM engagement and economic growth is uncertain
  - The balance between security, cost, and convenience
  - Preferences for user data storage are unexplored
- Continued harmoniation of regulatory regimes
- Alleviating compliance burdens/issues of SMEs via education and consultation measures
- Facilitate platform interoperability through the discussion and promotion of industry standards
  - Host or assist with the creation of PDS-specific industry conferences and events where standards and interoperability can be further promoted
  - Act as the hub for platform and ecosystem discussions to reduce information asymmetry and coordination problems
- Engage the industry to push for standardised terminology, concept and attributes of PDSs
- Help PDS providers reach a broad user-base, through:
  - Public procurement programs
  - Initiating dialogues with Telecoms
  - Following Apple's HealthKit
- Connect PDS providers to other personal data stakeholders through conferences and networking events
- Connect PDS providers with each other in order to foster the exchange of ideas; of particular interest is the critical mass issue in the context of a double-sided market
- Make funding sources widely visible and simple to understand

[131] Chell and Baines, "Networking, entrepreneurship and microbusiness behaviour", 2000, pp. 195–215.
[132] Jennings, *Statement on the Court of Auditors Report on FP7*, 2013.

Bibliography

Note: References are listed in alphabetical order by author.

Akerlof, George A. “The Market for “Lemons”: Quality Uncertainty and the Market Mechanism”. In: *The Quarterly Journal of Economics* 84.3 (Aug. 1970), pp. 488–500 (cit. on p. 2).

Alexandru, Plesea Doru, Maiorescu Irina, and Cîrstea Alice. “Consumers Attitude towards Consumer Protection in the Digital Single Market, as Reflected by European Barometers”. In: *The AMFITEATRU ECONOMIC journal* 36.16 (2014). url: http://www.amfiteatrueconomic.ro/temp/Article_1291.pdf (visited on 05/10/2015) (cit. on p. 2).

Aliprandi, Simone. “Interoperability and open standards: the key to a real openness”. In: *International Free and Open Source Software Law Review* 3.1 (Sept. 30, 2011), pp. 5–24. issn: 18776922. doi: 10.5033/ifosslr.v3i1.53. url: http://www.ifosslr.org/ifosslr/article/view/53/105 (visited on 05/12/2015) (cit. on p. 23).

Alstyne, Thomas R., Geoffrey Eisenmann, and Marshall W. Van Parker. *Strategies for Two-Sided Markets*. Harvard Business Review. 2006. url: https://hbr.org/2006/10/strategies-for-two-sided-markets (visited on 05/20/2015) (cit. on p. 42).

Article 29 Working Party. *Annex: Health Data in Apps and Devices*. 2015. url: http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2015/20150205_letter_art29wp_ec_health_data_after_plenary_annex_en.pdf (visited on 05/12/2015) (cit. on p. 16).

ASIP. *La e-sante, secteur de croissance au service de notre systeme de sante*. url: http://esante.gouv.fr/asip-sante/espace-presse/communiques-de-presse/la-e-sante-secteur-de-croissance-au-service-de-notre (visited on 05/25/2015) (cit. on p. 34).

Bell, Beverly and Kelly Thornton. “From promise to reality: achieving the value of an EHR”. In: *Healthcare Financial Management: Journal of the Healthcare Financial Management Association* 65.2 (Feb. 2011), pp. 50–56. issn: 0735-0732 (cit. on p. 13).

Boston Consulting Group. *The Value of Our Digital Identity*. Liberty Global, Inc., 2012. url: http://www.libertyglobal.com/PDF/public-policy/The-Value-of-Our-Digital-Identity.pdf (cit. on pp. 5, 10, 12, 28, 36).

— *The Value of Our Digital Identity*. Liberty Global, Inc., 2012, p. 56. url: http://www.libertyglobal.com/PDF/public-policy/The-Value-of-Our-Digital-Identity.pdf (cit. on p. 29).

— *The Value of Our Digital Identity*. Liberty Global, Inc., 2012, p. 3. url: http://www.libertyglobal.com/PDF/public-policy/The-Value-of-Our-Digital-Identity.pdf (cit. on p. 29).

— *The Value of Our Digital Identity*. Liberty Global, Inc., 2012, p. 41. url: http://www.libertyglobal.com/PDF/public-policy/The-Value-of-Our-Digital-Identity.pdf (cit. on p. 32).

Brill, Julie. “Big Data and Consumer Privacy: Identifying Challenges, Finding Solutions”. Public Address. Woodrow Wilson School of Public and International Affairs - Princeton University, Feb. 20, 2014 (cit. on pp. 11–13).

Business Intelligence. *Cloud Storage Costs - BI Insight*. Business Intelligence. June 2014. url: http://businessintelligence.com/bi-insights/cloud-storage-costs/ (visited on 05/20/2015) (cit. on p. 23).

BUSINESSMODELINNOVATIONMATTERS. *Comparing Facebook and Google Business Models | Understanding Business Models*. Apr. 18, 2012. url: http://bmimatters.com/2012/04/18/comparing-facebook-and-google-business-models/ (visited on 05/13/2015) (cit. on p. 4).

Cassano, Jay. *What Are Smart Contracts? Cryptocurrency's Killer App*. Co.Labs. Sept. 17, 2014. url: http://www.fastcolabs.com/3035723/app-economy/smart-contracts-could-be-cryptocurrencys-killer-app (visited on 05/12/2015) (cit. on p. 25).

Cavoukian, Ann and Shane Green. *Privacy by Design and the Emerging Personal Data Ecosystem*. Ontario, Canada, Oct. 2012. url: https://www.ipc.on.ca/images/Resources/pbd-pde.pdf (cit. on p. 4).

Cavoukian, Ann and Drummond Reed. “Big Privacy: Bridging Big Data and the Personal Data Ecosystem through Privacy by Design”. In: *Information and Privacy Commissioner, Ontario, Canada: Retrieved from http://www. privacybydesign. ca/index. php/paper/big-privacy* (2013). url: https://www.ipc.on.ca/site_documents/PbDBook-From-Rhetoric-to-Reality-ch3.pdf (visited on 03/30/2015) (cit. on p. 2).

Chell, Elizabeth and Susan Baines. “Networking, entrepreneurship and microbusiness behaviour”. In: *Entrepreneurship & Regional Development* 12.3 (July 1, 2000), pp. 195–215. issn: 0898-5626. doi: 10.1080/

089856200413464. url: http://dx.doi.org/10.1080/089856200413464 (visited on 05/21/2015) (cit. on p. 58).

Commission, European. *A Digital Single Market Strategy for Europe*. May 6, 2015. url: http://ec.europa.eu/priorities/digital-single-market/docs/dsm-communication_en.pdf (visited on 05/19/2015) (cit. on p. 15).

— *Data Protection Day 2015: Concluding the EU Data Protection Reform essential for the Digital Single Market*. Brussels: European Commission, Jan. 28, 2015. url: http://europa.eu/rapid/press-release_MEMO-15-3802_en.htm (visited on 05/25/2015) (cit. on pp. 15, 18).

Consolidated Version of the Treaty on the Functioning of the European Union. art. 168, 2008 O.J. C 115/47 (cit. on p. 20).

Council of the EU. *Data protection: Council agrees on general principles and the "one stop shop" mechanism - Consilium*. Mar. 13, 2015. url: http://www.consilium.europa.eu/en/press/press-releases/2015/03/13-data-protection-council-agrees-general-principles-and-one-stop-shop-mechanism/ (visited on 05/10/2015) (cit. on p. 18).

CSA. *Les Français et la protection des données personnelles*. CSA, 2014. url: http://www.csa.eu/multimedia/data/sondages/data2014/opi20140123-les-francais-et-la-protection-des-donnees-personnelles.pdf (cit. on p. 57).

Ctrl-Shift. *Personal Information Management Systems: An analysis of an emerging market*. Strand, London: Ctrl-Shift, June 2014. url: http://www.nesta.org.uk/sites/default/files/personal_information_management_services.pdf (cit. on pp. 34, 36, 37).

Davos, L.S. "The Snowden effect". In: *The Economist* (Jan. 24, 2014). issn: 0013-0613. url: http://www.economist.com/blogs/babbage/2014/01/internet-governance (visited on 05/10/2015) (cit. on pp. 2, 9).

EDPS. *Mobile Health: Reconciling Technological Innovation with Data Protection*. Opinion 1/2015. Brussels: European Data Protection Supervisor, May 21, 2015. url: https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2015/15-05-21_Mhealth_EN.pdf (visited on 05/23/2015) (cit. on p. 16).

Eisma, Franco. *PDS Conceptual Architecture*. May 20, 2015 (cit. on p. 20).

EMC. *EMC Privacy Index*. 2014. url: http://www.emc.com/campaign/privacy-index/index.htm (visited on 05/09/2015) (cit. on pp. 32, 36).

European Commission. *A Digital Single Market Strategy for Europe*. COM(2015) 192 final. Brussels: European Commission. May 2015. url: http://ec.europa.eu/priorities/digital-single-market/docs/dsm-communication_en.pdf (visited on 05/19/2015) (cit. on p. 2).

— *COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS: Towards a thriving data-driven economy*. Brussels. COM(2014) 442 final. July 2, 2014 (cit. on pp. 2, 10).

— *Comparing the organisation of health systems, Health Systems Performance Assessment*. url: http://ec.europa.eu/health/systems_performance_assessment/health_systems_organisation/comparing_organisation/index_en.htm (visited on 05/12/2015) (cit. on p. 18).

— *Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)*. Jan. 25, 2012. url: http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf (cit. on p. 15).

— *Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)*. art. 9, pg. 45. Jan. 25, 2012. url: http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf (cit. on pp. 15, 17).

— *Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)*. art. 7, pg. 45. Jan. 25, 2012. url: http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf (cit. on p. 17).

European Parliament and Council. "DIRECTIVE 2011/24/EU OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 9 March 2011 on the application of patient's rights in cross-border healthcare". In: *Official Journal of the European Union L 88/45* (Mar. 2011) (cit. on p. 17).

European Parliament and Council. "DIRECTIVE 2011/24/EU OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 9 March 2011 on the application of patient's rights in cross-border healthcare". In: *Official Journal of the European Union L 88/45* (Mar. 2011). Article 4(f), pg. 56 (cit. on p. 17).

Forum, World Economic and The Boston Consulting Group. *Rethinking Personal Data: Strengthening Trust*. Geneva, Switzerland: World Economic Forum, May 2012 (cit. on p. 2).

— *Rethinking Personal Data: Strengthening Trust*. Geneva, Switzerland: World Economic Forum, May 2012, p. 23 (cit. on p. 36).

Fraser, B. *Site Security Handbook*. Sept. 1997. url: https://www.ietf.org/rfc/rfc2196.txt (cit. on p. 23).

Glatz, Florian. *What's a Smart Contract? In search of a consensus*. Medium. Dec. 11, 2014. url: https://medium.com/@heckerhut/whats-a-smart-contract-in-search-of-a-consensus-c268c830a8ad (visited on 05/12/2015) (cit. on p. 25).

Google. *Using OAuth 2.0 to Access Google APIs*. May 15, 2015. url: https://developers.google.com/identity/protocols/OAuth2 (cit. on p. 24).

Grant, Elaine. *The promise of big data*. Harvard School of Public Health. 2012. url: http://www.hsph.harvard.edu/news/magazine/spr12-big-data-tb-health-costs/ (visited on 05/10/2015) (cit. on p. 13).

GSMA and PricewaterhouseCoopers. *Socio-economic impact of mHealth: An assessment report for the European Union*. June 2013. url: http://www.gsma.com/connectedliving/socio-economic-impact-of-mhealth-an-assessment-report-for-the-european-union/ (visited on 05/09/2015) (cit. on pp. 34, 36).

Haddadi, Hamed et al. "Personal Data: Thinking Inside the Box". In: (Jan. 20, 2015). arXiv: 1501.04737. url: http://arxiv.org/abs/1501.04737 (visited on 05/10/2015) (cit. on pp. 2, 9, 12, 17, 35, 55).

Holmlöv, P.G. and Karl-Erik Wärneryd. "Adoption and Use of Fax in Sweden". In: *Modelling the Innovation: Communications, Automation and Information Systems, Proceedings of the IFIP TC7 Conference on Modelling the Innovation: Communications, Automation and Information Systems*. Rome, Italy, Mar. 1990 (cit. on p. 42).

Hudson, Alex. "The age of information overload". In: *BBC* (Aug. 14, 2012). url: http://news.bbc.co.uk/1/hi/programmes/click_online/9742180.stm (visited on 05/14/2015) (cit. on p. 11).

Interview with Qiy Foundation. In collab. with Ad van Loon and Marcel van Galen. May 15, 2015 (cit. on p. 25).

Jennings, Michael. *Statement on the Court of Auditors Report on FP7*. June 7, 2013. url: http://ec.europa.eu/research/index.cfm?pg=newsalert&year=2013&na=na-070613 (cit. on p. 58).

Johnson, Matt, K. Lithgo, and T. Price. "OC-080 Ibd-Sshamp (Supported, Self help and Management Programme); UK'S first Internet based Remote Management System for Managing Stable IBD". In: *Gut* 62.1 (2013). doi: 10.1136/gutjnl-2013-304907.079 (cit. on p. 49).

Kraut, Robert et al. "Internet Paradox: A Social Technology That Reduces Social Involvement and Psychological Well-Being?" In: *American Psychologist* 53.9 (1998) (cit. on p. 42).

Kuneva, Meglena. *Keynote Speech*. Roundtable on Online Data Collection, Targeting and Profiling, Brussels. Mar. 31, 2009. url: http://europa.eu/rapid/press-release_SPEECH-09-156_en.htm (cit. on p. 2).

l'Assurance Maladie. *Cout des ALD en 2009*. 2015. url: http://www.ameli.fr/l-assurance-maladie/statistiques-et-publications/donnees-statistiques/affection-de-longue-duree-ald/cout/cout-des-ald-en-2009.php (visited on 05/25/2015) (cit. on p. 34).

Lewis, Daniel Jacob. *Radar Charts Illustrating PDS Ecosystem*. May 2015 (cit. on p. 4).

Manyika, James et al. *Open Data: Unlocking Innovation and Performance with Liquid Information*. McKinsey & Company, Oct. 2013. url: http://www.mckinsey.com/insights/business_technology/open_data_unlocking_innovation_and_performance_with_liquid_information (cit. on pp. 2, 5).

Martens, Bertin. "What does economic research tell us about cross-border e-commerce in the EU Digital Single Market?" In: *Available at SSRN 2265305* (2013). url: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2265305 (visited on 05/10/2015) (cit. on p. 2).

Millman, Rene. *Google price cuts see cloud costs fall by 10 per cent | Cloud Pro*. Oct. 2014. url: http://www.cloudpro.co.uk/cloud-essentials/4515/google-price-cuts-see-cloud-costs-fall-by-10-per-cent (visited on 05/12/2015) (cit. on p. 23).

Moazed. *7 Strategies for Solving the Chicken and Egg Problem as a Startup*. The Huffington Post. 2015. url: http://www.huffingtonpost.com/alex-moazed/7-strategies-for-solving-_b_6809384.html (visited on 05/20/2015) (cit. on p. 42).

Moore, Geoffrey A. *Crossing the Chasm: Marketing and Selling Technology Products to Mainstream Customers (Capstone Trade)*. Revised Edition. Capstone, Aug. 1998. isbn: 978-1841120638 (cit. on p. 39).

Mydex CIC. *The Case for Personal Information Empowerment: The rise of the Personal Data Store*. 2010. url: https://mydex.org/wp-content/uploads/2010/09/The-Case-for-Personal-Information-Empowerment-The-rise-of-the-personal-data-store-A-Mydex-White-paper-September-2010-Final-web.pdf (visited on 05/10/2015) (cit. on pp. 9, 11, 25).

Nicole Denjoy. *eHealth Stakeholder Group report Perspectives and Recommendations on Interoperability*. Mar. 2014. url: ec.europa.eu/information_society/newsroom/cf/dae/document.cfm?doc_id=5168 (cit. on p. 25).

OAuth. *An open protocol to allow secure authorization in a simple and standard method from web, mobile and desktop applications*. url: http://oauth.net (cit. on p. 24).

OECD. *Data Driven Innovation for Growth and Well-being*. OECD. Oct. 2014. url: http://www.oecd.org/sti/inno/data-driven-innovation-interim-synthesis.pdf (visited on 05/10/2015) (cit. on pp. 11, 13).

Open Identity Exchange. *OIX Trust Frameworks*. 2015. url: http://openidentityexchange.org/resources/trust-frameworks (visited on 05/12/2015) (cit. on p. 25).

Parliament, European. *GDPR - Draft*. Mar. 12, 2014. url: http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P7-TA-2014-0212+0+DOC+XML+V0//EN (visited on 05/21/2015) (cit. on p. 16).

Parr, Ben. *The Google Revenue Equation, and Why Google's Building Chrome OS*. July 2011. url: http://mashable.com/2009/07/11/google-equation/ (visited on 05/13/2015) (cit. on p. 4).

Patients Know Best. *Welcome to the world's first patient-controlled medical record*. Patients Know Best: Manage Your Health. 2015. url: https://www.patientsknowbest.com (visited on 04/05/2015) (cit. on p. 3).

Pearson, Siani and Marco Casassa Mont. "Sticky policies: an approach for managing privacy across multiple parties". In: *Computer* 44.9 (2011), pp. 60–68. url: https://documents.epfl.ch/users/a/ay/ayday/www/mini_project/Sticky%20Policies.pdf (visited on 05/12/2015) (cit. on p. 26).

Pijl, Patrick van der. *Facebooks' Business Model Visualized - Business Model Innovation Hub*. Mar. 29, 2011. url: http://businessmodelhub.com/forum/topics/facebooks-business-model (visited on 05/13/2015) (cit. on p. 4).

Podesta, John et al. *Big Data: Seizing Opportunities, Preserving Values*. White House Report. Executive Office of the President, May 2014 (cit. on pp. 11, 12).

President's Council of Advisors on Science and Technology. *BIG DATA AND PRIVACY: A TECHNOLOGICAL PERSPECTIVE*. May 2014. url: https://www.whitehouse.gov/sites/default/files/microsites/ostp/PCAST/pcast_big_data_and_privacy_-_may_2014.pdf (cit. on p. 25).

Privacy Rights Clearinghouse. *Chronology of Data Breaches*. Apr. 20, 2005. url: http://www.privacyrights.org/data-breach (visited on 05/19/2015) (cit. on p. 9).

Progress Consulting S.r.l. and Living Prospects Ltd. *The management of health systems in the EU Member States - The role of local and regional authorities*. Commissioned Study. Brussels: European Union. 2012. doi: 10.2863/83500. url: http://cor.europa.eu/en/documentation/studies/Documents/health-systems/health-systems-en.pdf (visited on 05/10/2015) (cit. on p. 13).

PwC. *Issue 3: Balancing privacy and convenience*. PwC. 2015. url: http://www.pwc.com/us/en/health-industries/top-health-industry-issues/privacy.jhtml (visited on 05/10/2015) (cit. on pp. 13, 15).

Raghupathi, Wullianallur and Viju Raghupathi. "Big data analytics in healthcare: promise and potential". In: *Health Information Science and Systems* 2.1 (Feb. 7, 2014), p. 3. issn: 2047-2501. doi: 10.1186/2047-2501-2-3. url: http://www.hissjournal.com/content/2/1/3/abstract (visited on 05/12/2015) (cit. on p. 13).

Respect Network. *Respect Trust Framework*. Open Identity Exchange. url: http://openidentityexchange.org/trust-frameworks/respect-trust-framework/ (visited on 05/10/2015) (cit. on p. 15).

Ries, Eric. *The Lean Startup: How Today's Entrepreneurs Use Continuous Innovation to Create Radically Successful Businesses*. First Edition edition. New York: Crown Business, Sept. 13, 2011. 336 pp. isbn: 9780307887894 (cit. on p. 26).

Robinson, Neil et al. *Review of the EU Data Protection: Summary*. Information Commissioner's Office. London: Information Commissioner's Office, May 2009. url: https://ico.org.uk/media/about-the-ico/documents/1042347/review-of-eu-dp-directive-summary.pdf (visited on 05/10/2015) (cit. on p. 16).

Rochet, Jean-Charles and Jean Tirole. "Platform Competition in Two-Sided Markets". In: *Journal of the European Economic Association* 1.4 (June 1, 2003), pp. 990–1029. issn: 1542-4774. doi: 10.1162/

154247603322493212. url: http://onlinelibrary.wiley.com/doi/10.1162/154247603322493212/abstract (visited on 05/20/2015) (cit. on p. 41).

Rogers, Everett. *Diffusion of Innovations*. 5th. Free Press, Aug. 2003. isbn: 978-0743222099 (cit. on pp. 39, 42).

Rubens, Paul. *Can Cloud Storage Costs Fall to Zero? - EnterpriseStorageForum.com*. Aug. 2014. url: http://www.enterprisestorageforum.com/storage-management/can-cloud-storage-costs-fall-to-zero-1.html (visited on 05/12/2015) (cit. on p. 23).

Sheehan, Mark. "Can Broad Consent be Informed Consent?" In: *Public Health Ethics* 4.3 (Nov. 1, 2011), pp. 226–235. issn: 1754-9973, 1754-9981. doi: 10.1093/phe/phr020. url: http://phe.oxfordjournals.org/content/4/3/226 (visited on 05/21/2015) (cit. on p. 17).

Spiekermann, Sarah and Alexander Novotny. "A vision for global privacy bridges: technical and legal measures for international data markets". In: *Computer Law & Security Report* 31.2 (Apr. 1, 2015), p. 181. issn: 0267-3649. doi: 10.1016/j.clsr.2015.01.009 (cit. on p. 26).

Szabo, Nick. *Smart Contracts: Building Blocks for Digital Markets*. 1996. url: http://szabo.best.vwh.net/smart_contracts_2.html (visited on 05/12/2015) (cit. on p. 25).

Taylor, Chris. *Apple's Business Model Is Backwards — And It Works Like Crazy*. Oct. 23, 2013. url: http://mashable.com/2013/10/23/apple-free-software-expensive-hardware/ (visited on 05/13/2015) (cit. on p. 4).

Twitter. *OAuth: Using OAuth*. 2015. url: https://dev.twitter.com/oauth/overview/introduction (cit. on p. 24).

Utterback, James M. *Dominant Designs and the Survival of Firms*. 1994 (cit. on p. 44).

Vishwanath, Siddharth et al. *Touching Lives through Mobile Health: Assessment of the Global Market Opportunity*. 2012 (cit. on p. 36).

Vodafone. *Rethinking Personal Data: Vodafone's perspective on creating value through end-user control, transparency and trust*. 2011. url: http://www.vodafone.com/content/dam/vodafone/about/privacy/vodafone_rethinking_personaldata.pdf (cit. on p. 57).

Walker, Joseph. *Data Mining to Recruit Sick People*. WSJ. Dec. 17, 2013. url: http://www.wsj.com/articles/SB10001424052702303722104579240140554518458 (visited on 05/10/2015) (cit. on p. 11).

Wittes, Benjamin. *Databuse: Digital Privacy and the Mosaic*. The Brookings Institution. Apr. 1, 2011. url: http://www.brookings.edu/research/papers/2011/04/01-databuse-wittes (visited on 05/10/2015) (cit. on p. 12).

World Economic Forum and The Boston Consulting Group. *Unlocking the Value of Personal Data: From Collection to Usage*. Geneva, Switzerland, 2013. url: http://www3.weforum.org/docs/WEF_IT_UnlockingValuePersonalData_CollectionUsage_Report_2013.pdf (cit. on p. 2).

Yaraghi, Niam. *A Sustainable Business Model for Health Information Exchange Platforms: The Solution to Interoperability in Health Care IT*. Jan. 30, 2015. url: http://www.brookings.edu/research/papers/2015/01/30-sustainable-business-model-health-information-exchange-yaraghi (cit. on p. 24).