Panel

Removing the barriers for personal data management

Bharosa, Nitesh; Luitjens, Steven; Van Wijk, Remco; Pardo, Theresa

DOI
10.1145/3209281.3209327

Publication date
2018

Document Version
Final published version

Published in
Proceedings of the 19th Annual International Conference on Digital Government Research

Citation (APA)
Bharosa, N., Luitjens, S., Van Wijk, R., & Pardo, T. (2018). Panel: Removing the barriers for personal data management. In C. C. Hinnant, & A. Zuiderwijk (Eds.), *Proceedings of the 19th Annual International Conference on Digital Government Research: Governance in the Data Age, DG.O 2018* [a125] Association for Computing Machinery (ACM). https://doi.org/10.1145/3209281.3209327

Panel: Removing the barriers for personal data management

Nitesh Bharosa
Delft University of Technology
The Netherlands

Steven Luitjens
Ministry of the Interior & Kingdom Relations of the Netherlands

Remco van Wijk
Cleverbase
The Netherlands

Theresa Pardo
Center for Technology in Government, University at Albany
USA

ABSTRACT

In our data-driven society, both public and private organisations are struggling with issues regarding privacy and personal data. On the one hand, consumers are required to hand over more and more personal data in return for (free) online services. On the other hand, regulations increasingly demand data minimisation and informed consent. Personal data management is often proposed as a human centric design philosophy that should ultimately allow consumers to gain back control over, and insight in, the processing of personal data. This signals a transition from provider centric to human centric e-societies. The **goal** of this panel is to explore which roles government, business and knowledge institutes can play in order to enable personal data management. What can and should these parties do? And what should consumers - the users of online services - do?

CSS CONCEPTS

• Social and professional topics→Governmental regulations;

KEYWORDS

Personal data management, eIDs, information processing, General Data Protection Act.

ACM Reference Format

N. Bharosa, S. Luitjens, R. van Wijk, T. Pardo. 2018. *Panel: Removing the barriers for personal data management.* In Proceedings of 19th Annual International Conference on Digital Government Research (dg.o'18), Anneke Zuiderwijk and Charles C. Hinnant (Eds.). ACM, New York, NY, USA, 3 pages.

1 INTRODUCTION

You have probably already heard the phrase 'data is the new oil'. As powerful as this sounds, this analogy is an understatement. While oil is a finite resource, data is in fact infinitely useful, reusable, transferable and storable. Billions of people constantly share data as part of social interactions and the consumption of business or public services. The use of smartphones and the internet have made data abundant, pervasive and useful for many organisations. Data – with the ease and in the quantities it is available today – is, in fact, an new commodity. Moreover, the rules around how data is stored, exchanged, processed and used by public and private organisations are still being written. However – fueled by a long list of data breaches – it becomes more and more unclear who exactly uses our personal data, how often and for what reasons. Once it is harvested, personal data is exchanged between multiple organisations, without the consent of individuals.

Giovanni Buttarelli, the European Data Protection Supervisor (EDPS) [1], said: "Our online lives currently operate in a provider-centric system, where privacy policies tend to serve the interests of the provider or of a third party, rather than the individual. Using the data they collect, advertising networks, social network providers and other corporate actors are able to build increasingly complete individual profiles. This makes it difficult for individuals to exercise their rights or manage their personal data online. A more human-centric approach is needed which empowers individuals to control how their personal data is collected and shared."

Figure 1 provides an illustration of the provider centric e-society in which personal data is scattered across various public and private organisations.

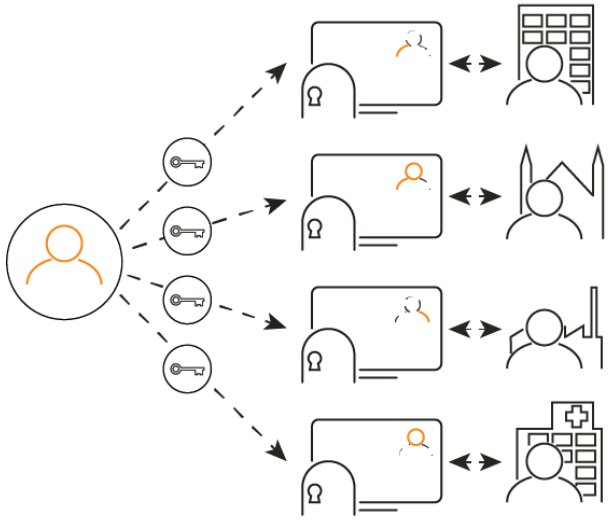

Figure 1: Provider centric e-society

dg.o '18, May 30-June 1, 2018, Delft, Netherlands

ACM ISBN 978-1-4503-6526-0/18/05.
https://doi.org/10.1145/3209281.3209327

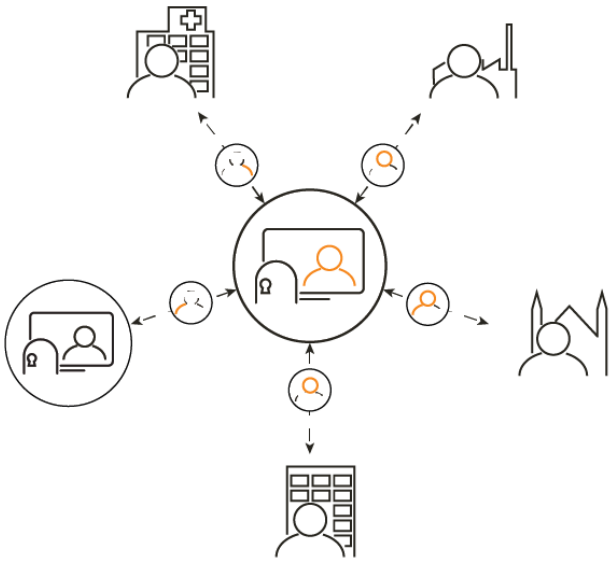

Figure 2: Personal data management in a human centric e-society

Several developments including recent European regulations and personal data breaches such as the Facebook – Cambridge Analytica scandal have strengthened the call for a more human centric e-society. One conceptualization of a more human centric approach is that of personal data management. Simply put, personal data management means that individuals (natural persons) can themselves store their personal data in secure online data storage systems and decide when and with whom to share personal data for a predefined goal. The data can then only be accessed and processed by entities that are (by user and/or law) allowed to do so for a predefined purpose. Emerging technologies like online personal data vaults (also known as data stores) play an important part in realising personal data management. A variety of designs and business models currently exist. However, they all share the idea of strengthening fundamental rights of individuals in the digital world.

Figure 2 provides an illustration of a more human centric e-society. Ideally, the transition towards human centricity and personal data management should allow for more tailored service delivery towards citizens. It could open up new industries and business models for serving citizens since they would be able to provide service providers access to their 'complete and up to data profile', instead of giving fragmented parts of the puzzle (since the data is scattered across many closed organizational systems). So, what should be done to guide this major societal transition towards the human centric model?

From a regulatory perspective, the foundations have been laid down in Europe for the more human-centric approach. On the one hand, the General Data Protection Regulation (GDPR) provides a framework for increased transparency, powerful rights of access and data portability, giving individuals more control over their data. The revised Payment Service Directive (PSD2) proposes similar rights, particularity when it comes to financial data. One the other hand, the eIDAS (electronic IDentification, Authentication and trust Services) regulation provides standards for electronic identification and trust services for electronic transactions in the European Single Market. The eIDAS regulation underlines the obligation to recognise electronic identification means should relate only to those means the identity assurance level of which corresponds to the level equal to or higher than the level required for the online service in question. In addition, that obligation should only apply when the public sector body in question uses the assurance level 'substantial' or 'high' in relation to accessing that service online. Assurance levels should characterise the degree of confidence in electronic identification means in establishing the identity of a person, thus providing assurance that the person claiming a particular identity is in fact the person to which that identity was assigned. The assurance level depends on the degree of confidence that electronic identification means provides in claimed or asserted identity of a person taking into account processes (for example, identity proofing and verification, and authentication), management activities (for example, the entity issuing electronic identification means and the procedure to issue such means) and technical controls implemented.

However, digital identities with a high assurance level are widely recognized as one of the major necessities for reaching the next level in e-society (e-government, e-business, e-health etc.). Identities enables many societal transactions, making strong identity systems critical to the function of society as a whole. Current identity systems are limiting innovation and well as secure and efficient service delivery in all parts of the e-society. In these systems, natural persons have limited access to easy to use tools that enable them to use verified digital identities for placing qualified signatures and express consent in a formal information process. In many business and government processes, paper statements still play an essential part of the processes, and automation is limited to the transport of scanned documents. For example, to apply for a mortgage in the Netherlands, an employer's declaration is required on paper with either a business stamp or a letter with a "wet signature" stating that the company does not possess a business stamp. Citizens often receive letters at their home address in order to facilitate digital processes, since for many parties this is a more trustworthy addressing system than for example email. An example is the pre-completed tax return process in the Netherlands. Although such paper based loops help satisfy requirements for authentication and authorisation, they are costly and pose risks such as undetectable data breach (e.g., letter opened by someone else who then disposes it). Alternatively, the use of e-mail carries the risk of social engineering and identity fraud. When funds are available, some organisations invest in secured digital portals and expect that persons use these in formal interactions. Yet, in practice, many users do not even know the portal exists until sanctions follow. Examples include the use of portals of the Office of Education in the Netherlands [2] and the use of the digital post-box of the Dutch Government [3] .

To sum up, digital identities with high level of assurance is required for moving towards a more human centric e-society by enabling:

(1) **Personal data management:** identity based control over the exchange and processing of any information relating to

an identified or identifiable natural person. Tools such as personal digital vaults can be used for personal data management.

(2) **Qualified information exchange:** digital interactions in which all the involved identities and theirs actions satisfy the requirements and guidelines stated in applicable regulations. Multiple building blocks are required for qualified information exchange, including electronic IDs (eIDs), data specifications, processes, technical protocols and support. When it comes to eIDs, the eIDAS regulation (which is effective for all EU member states) introduces the notion of qualified trust service providers, indicating requirements and obligations that ensure high-level security of whatever qualified trust services and products are used or provided. The goal is to enhance in particular the trust of consumers and enterprises in the internal market and to promote the use of trust services and products.

(3) **Efficient, high quality value added service delivery:** organizations can streamline and automate more processes, without the delays and inefficiencies that result from working with physical identities or digital identities that require verifications. Reliance on physical identity protocols and verification channels (e.g. bring your passport to our front desk) introduces inefficiency and errors to these processes. Moreover, if individuals have (a copy) of all their personal data, it would be easier for service providers to request a copy of all the personal data in order to provide more tailored service offerings.

2 KEY QUESTIONS

Guided by a moderator, this panel will discuss several questions regarding personal data management, including:

- What are the grand challenges for enabling personal data management?
- How can we address the privacy paradox and as well as the use of social media as open data for governmental processes (e.g. for compliance or fraud detection)?
- How can citizens be made more aware of the unintended and maybe even unfair use of personal data?
- What are strong 'use cases' for stimulating personal data management?
- What kind of societal or business opportunities can be opened up by personal data management?
- Which building blocks are needed for personal data management?
- If digital identities with high level of assurance are widespread and available for everyone, what else is needed for personal data management?
- What about tech: the user apps, tools and infrastructure needed for qualified information exchange?
- Which roles can government, business and knowledge institutes play in realising personal data management?
- What should citizens – the users of online services – do?

The panel will also take questions from the audience.

3 PANELIST

The panel consist of representatives from government, business and knowledge institutes allowing us to capture various perspectives on personal data management. The participants invited to join the panel are:

Steven Luitjens - Director of Information Society and Government at Ministry of the Interior and Kingdom Relations of the Netherlands. He deals with questions on what digitization does to society and hopes to strengthen the confidence of the citizen in the digital government. His department has recently published a green paper on the subject of personal data management. Prior to this panel, Steven will provide the keynote speech on personal data management.

Remco van Wijk - Chief Technology Officer of Cleverbase, a Qualified Trust Service Provider in the Netherlands. Remco is an expert on the design of inter-organisational information systems and has co-authored several publications on this topic. His latest book – Qualified information exchange[1] – discusses the building blocks required for qualified information exchange in the 21st century.

Theresa Pardo - Director of the Center for Technology in Government (CTG) at the University at Albany. CTG works closely with multi-sector and multi-disciplinary teams from the U.S. and around the world to carry out applied research and problem-solving projects focused on the intersections of policy, management, and technology in the governmental context.

The panel will be moderated by **Nitesh Bharosa**. Nitesh is senior researcher at Delft University of Technology and head of research and development at Smart Data Company. His research interests include digitalisation, personal data management and the design of inter-organisational information systems in a public-private context (e.g. business to government reporting and sector supervision). Nitesh has published multiple books and peer reviewed articles on this topics, 'Challenging the Chain: Governing the Automated Exchange and Processing of Business Information[2].

REFERENCES

[1] EDPS. 2016. Towards a new reality: Taking back control of our online identities - European Data Protection Supervisor. (2016). https://edps.europa.eu/press-publications/press-news/press-releases/2016/towards-new-reality-taking-back-control-our-online

[2] NOS. 2017. Aanmaningen, boetes: mensen missen massaal digitale post van overheid. (2017). https://nos.nl/artikel/2191693-aanmaningen-boetes-mensen-missen-massaal-digitale-post-van-overheid.html

[3] NOS. 2017. 'Wie kijkt er nou op MijnDUO?'. (2017). https://nos.nl/op3/artikel/2165437-wie-kijkt-er-nou-op-mijnduo.html

[1] http://qualifiedinformationexchange.com/

[2] https://www.iospress.nl/book/challenging-the-chain/