Privacy-ABC Technologies, Personal Data Ecosystem, and Business Models

A feasibility study report

Fatbardh Veseli, Welderufael B. Tesfay

Editors:	*Welderufael B. Tesfay, Fatbardh Veseli (Goethe University Frankfurt)*
Reviewers:	*Jan Camenisch (IBM Research – Zurich), Robert Seidl (Nokia)*
Identifier:	*R2.1*
Type:	*Report*
Version:	*1.0*
Date:	*2015-01-09*
Status:	*Review*
Class:	*Public*

Abstract

This report presents a study on Privacy-ABC technologies in relation to Personal Data Ecosystem (PDE) management and business models around the two. First, we consider existing business models around PDE and investigate how they can be impacted if Privacy-ABC technologies would be adopted within their architecture. In this regard, we focus on two main concepts, namely on data brokerage, and Personal Data Ecosystem (PDE) management. With regard to data brokerage, we describe current practices for personal data collection and usage, and then identify potential benefits of using Privacy-ABC technologies for both users and data brokers. Next, we describe the concept of PDE management, describing its goals, main technologies and stakeholders. In particular, we focus on the Respect Network, which represents a concrete business model aiming to empower users with personal data economic benefits and control of their data. Second, we also consider the potential of Privacy-ABC technologies in creating new business models. In this regard, we identify two main domains, where we consider Privacy-ABC technologies have such a potential. One of them involves providing Privacy-ABC features as services in an identity ecosystem for different entities that want to outsource these processes, most notably token verification, inspection, and revocation. In addition, we suggest a privacy-enhanced method of online personalised advertisement, acknowledging the potential of Privacy-ABC technologies to both help advertisers improve the quality of targeted advertisements and at the same time provide a higher degree of privacy to the consumers.

The research leading to these results has received funding from the European Community's Seventh Framework Programme (FP7/2007-2013) under grant agreement n° 257782 for the project Attribute-based Credentials for Trust (ABC4Trust) as part of the "ICT Trust and Security Research" theme.

Members of the ABC4TRUST consortium

1.	Alexandra Institute AS	ALX	Denmark
2.	CryptoExperts SAS	CRX	France
3.	Eurodocs AB	EDOC	Sweden
4.	IBM Research – Zurich	IBM	Switzerland
5.	Johann Wolfgang Goethe-Universität Frankfurt	GUF	Germany
6.	Microsoft Belgium NV	MS	Belgium
7.	Miracle A/S	MCL	Denmark
8.	Nokia	NSN	Germany
9.	Computer Technology Institute and Press "Diophantus"	CTI	Greece
10.	Söderhamn Kommun	SK	Sweden
11.	Technische Universität Darmstadt	TUD	Germany
12.	Unabhängiges Landeszentrum für Datenschutz	ULD	Germany

***Disclaimer**: The information in this document is provided "as is", and no guarantee or warranty is given that the information is fit for any particular purpose. The above referenced consortium members shall have no liability for damages of any kind including without limitation direct, special, indirect, or consequential damages that may result from the use of these materials subject to any liability, which is mandatory due to applicable law.*

Copyright 2014 by Goethe University Frankfurt, and other partners of the consortium.

List of Contributors

Chapter	**Author(s)**
Executive Summary	Fatbardh Veseli
Chapter 1	Welderufael B. Tesfay, Fatbardh Veseli
Chapter 2	Fatbardh Veseli, Welderufael B. Tesfay
Chapter 3	Fatbardh Veseli
Conclusion	Fatbardh Veseli

Executive Summary

Personal data represent a valuable asset in today's sharing economy on the Internet. A number of businesses nowadays rely on data as a source of revenue, making personal data an important element in their business models. Privacy-enhancing Attribute-Based Credential (Privacy-ABC) technologies are tools that enable building identity management systems supporting both the interests users for privacy and of service providers for the desired identity services. The focus of this report is to understand the potential impact of Privacy-ABC technologies on existing business models, and to identify potential new business models that could arise with the adoption of Privacy-ABC technologies.

This document starts with a general overview of the main concepts of Privacy-ABC technologies and the main entities of the architecture of Privacy-ABC technologies, as defined in the ABC4Trust architecture deliverable [BIC+14]. Building on this, we draw relations between Privacy-ABC technologies and a number of business models that evolve around personal data. In particular, we describe how the adoption of Privacy-ABC technologies could affect existing business models. In this regard, we focus on data brokerage as a particular type of business evolving around personal data. We present a brief overview of the current practices of data brokers in collecting, analysing, and selling (services based on) personal data. In addition, we discuss the potential impacts of adopting Privacy-ABC technologies into the data brokerage approach, and identify a number of benefits of such an adoption for both data brokers and users.

Next, we present the innovative concept of Personal Data Ecosystem (PDE) management, which represents a landscape of companies and organizations that believe individuals should control their personal data. Here we identify some of the main technologies and stakeholders of the PDE, and describe the main goals of PDE management. We compare the existing "organizational-centric" approach of PDE management with a newer, "user-centric" approach. In this regard, we take a closer look at the Respect Network as a particular business model within the PDE, describing its relation to user's privacy, and discuss the potential of integrating Privacy-ABC technologies into the Respect Network architecture.

With regard to the potential for creating new business models, we identify two important domains. The first one describes a business model that focuses on providing some of the core features of Privacy-ABC technologies as services in the identity management ecosystem. The second domain relates to online advertisement, where we consider the potential of integrating Privacy-ABC technologies to improve both the privacy of the users and the quality of the targeted advertisement.

Table of Contents

Index of Figures

1. Introduction[1]

ABC4Trust has brought together industry, academia and others to address the federation and interchangeability of technologies that support trustworthy yet privacy-preserving Attribute-based Credentials (ABCs). Privacy-ABC technologies are an important building block of identity management systems, which enable the preservation of additional privacy in user's identity-related transactions with different services. Among the privacy features of Privacy-ABCs are the possibility these technologies bring to enable a holder (the User) to disclose a *minimal set of* credential *attributes* to services, perform *anonymous proofs* of possession of certain credentials or having attribute values matching certain criteria, while enabling *unlinkability* of identity-related transactions, when this is desired.

At the last stage of the project, we have made an effort to study how Privacy-ABCs can improve existing business models and allow the evolution of new ones. The study focuses on personal data ecosystem management, and attribute brokerage business aspects.

This chapter provides a brief overview of the main actors of the ABC4Trust architecture and their basic interactions, and some basic concepts behind Privacy-ABC technologies.

1.1 An Overview of the ABC4Trust Architecture

The ABC4Trust architecture consists of different entities. Each of these entities performs interactions with the relevant bodies in the architecture. The entities and their corresponding functionalities are discussed below.

As shown in Figure 1, the following five architectural entities can interact in the various possible scenarios:

- The *User* is at the centre of the picture, collecting *Credentials* from various Issuers and controlling which information from which credentials she presents to which verifiers. The human User is represented by her *User Agent*, a software component running either on a local device (e.g., on the User's computer or mobile phone) or remotely on a trusted cloud service. The User may own special hardware tokens to which credentials can be bound to improve security. In the identity management literature, the User is sometimes referred to as the requestor or the subject.
- An *Issuer* issues credentials to Users, thereby vouching for the correctness of the information contained in the credential with respect to the User to whom the credential is issued. Before issuing a credential, the Issuer may have to authenticate the User, which it may do using Privacy-ABCs, using a different online mechanism (e.g., username and password), or using out-of-band communication (e.g., by requiring the User to physically present herself at the Issuer's office). In the identity management literature, the Issuer is sometimes referred to as the identity provider or attributes authority.

[1] Sections 1.1 and 1.2 in this chapter are largely taken and slightly adapted from Chapter 2 of the ABC4Trust architecture deliverable [BIC+14]. The credits hereby go to the authors of that chapter and the reader is suggested to have a look at the original deliverable for more complete and further reading.

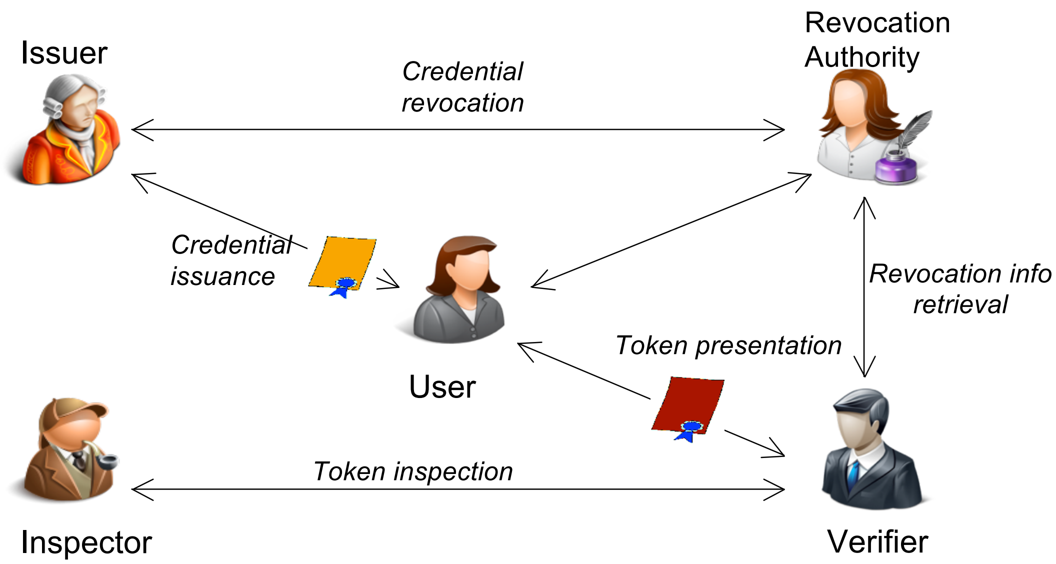

Figure 1: ABC4Trust architecture entities and their interactions

- A *Verifier* protects access to a resource or service that it offers by imposing restrictions on the credentials that Users must own and the information from these credentials that Users must present in order to access the service. The Verifier's restrictions are described in its presentation policy. The User generates from her credentials a presentation token that contains the required information and the supporting cryptographic evidence. In the identity management literature, the Verifier is sometimes also referred to as the relying party, the server, or the service provider. A brief overview of the interaction between the User and the Verifier is shown in Figure 2.

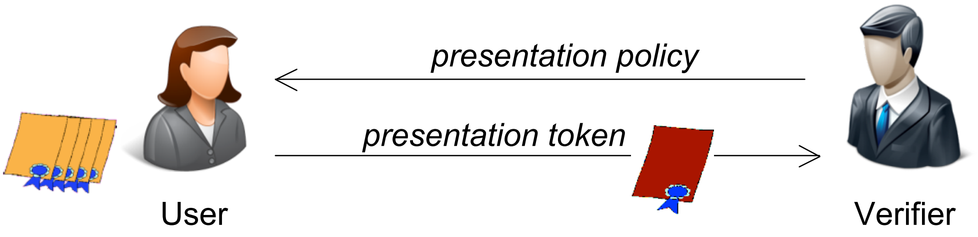

Figure 2: An overview of the presentation process

- A *Revocation Authority* is responsible for revoking issued credentials, so that these credentials can no longer be used to generate a presentation token. The use of a particular Revocation Authority may be imposed by the Issuer, in which case the revoked credentials cannot be used with any Verifier for any purpose, or by the Verifier, in which case the effect of the revocation is local to the Verifier and does not affect presentations with other Verifiers. Both the User and the Verifier must obtain the most recent revocation information from the Revocation Authority to generate, respectively verify, presentation tokens.
- An *Inspector* is a trusted authority who can, under specific circumstances, de-anonymize presentation tokens. To make use of this feature, the Verifier must specify in the

presentation policy the Inspector authority that should be able to recover specific attribute(s) should the predefined circumstances arise. The User is therefore aware of the de-anonymization possibility when the token is generated and actively participates to make this possible; therefore the User can make a conscious decision based on her trust in the Inspector.

In an actual deployment, some of the above roles may actually be fulfilled by the same entity or split among many. For example, an Issuer can at the same time play the role of Revocation Authority and/or Inspector, or an Issuer could later also be the Verifier of tokens derived from credentials that it issued.

1.2 Concepts of Privacy-ABCs

A *credential* is a certified container of attributes issued by an *Issuer* to a *User*. An attribute is described by the *attribute type*, determining the semantics of the attribute (e.g., first name), and the *attribute value*, determining its contents (e.g., John). By issuing a credential, the Issuer vouches for the correctness of the contained attributes with respect to the User. The User can then later use her credentials to derive *presentation tokens* that reveal *partial* information about the encoded attributes to a Verifier.

In a typical scenario (Figure 2) a Verifier announces in its *presentation policy* which credentials from which Issuers it accepts and which attributes from the credential(s) must be disclosed. The Verifier can cryptographically verify the authenticity of a received presentation token using the credential specifications and issuer parameters of all credentials involved in the presentation token. The Verifier must obtain the credential specifications and issuer parameters in a trusted manner, e.g., by using a traditional PKI to authenticate them or retrieving them from a trusted location.

To provide certified information to a Verifier (for authentication or an access decision), the User uses one or more of her credentials to derive a *presentation token* and sends it to the Verifier. A single presentation token can contain information from any number of credentials. The token can reveal a subset of the attribute values in the credentials (e.g., IDcard.firstname = "John"), prove that a value satisfies a certain predicate (e.g., IDcard.birthdate < 1993/01/01) or that two values satisfy a predicate (e.g., IDcard.lastname = creditcard.lastname).

The presentation token created in response to such a presentation policy consists of the *presentation token description,* containing a mechanism-agnostic description of the revealed information, and the *presentation token evidence,* containing opaque technology-specific cryptographic data in support of the token description.

Presentation tokens based on Privacy-ABCs may be unlinkable, meaning that Verifiers cannot tell whether two presentation tokens were derived from the same or from different credentials, and untraceable, so that Issuers cannot trace a presentation token back to the issuance of the underlying credentials. However, we have considered additional mechanisms so that, with the User's consent, it enables a dedicated third party to recover this link again (inspection).

In particular, the architecture has been designed to decompose future (reference) implementations of Privacy-ABC technologies, into sets of modules and specify the abstract functionality of these components in such a way that they are independent from the cryptographic mechanisms used underneath. The functional decomposition foresees possible architectural extensions to additional functional modules that may be desirable and feasible using future Privacy-ABC technologies or extensions of existing ones, so that new building blocks can be used, such as zero knowledge proofs, inspection, revocation, or signature schemes.

1.3 Organization of the document

This document is organized as follows. Chapter 2 provides an overview of existing data-related business models and the potential of integration of Privacy-ABC technologies into existing approaches, including data brokerage and personal data ecosystem management. We consider attributes to be essential data elements in existing data brokerage models, and consider therefore attribute brokerage synonymous to data brokerage in this context. Chapter 3 discusses new business models which may result from the adoption of Privacy-ABC technologies, including a discussion about Privacy-ABC features as services. In addition, this chapter studies at the potential of using Privacy-ABC technologies to provide a more effective and privacy-enhancing targeted online advertisement. Finally, Chapter 4 concludes the document and gives an outlook on the future work.

2. Personal Data Ecosystem management, Privacy-ABC technologies and existing business models

In this chapter, we provide two business models that are built around personal data. First, we present data brokerage and its current business model, describe data collection and usage methods, and identify the main categories of revenues for this type of business. In addition, we identify a number of points, where Privacy-ABC technologies could prove helpful to improve the effectiveness of current data brokerage approaches. Second, we describe the concept of Personal Data Ecosystem (PDE) management and take a closer look at one particular framework, namely the Respect Network, which is an example of a concrete business model focusing on fair relationships between users and (cloud) service providers. In this regard, we describe the business model of the Respect Network and its main features, and assess the potential of integrating Privacy-ABC technologies into this framework.

2.1 Data brokerage

There seems to be no unique definition of data brokerage [CCST13]. While the Oxford dictionary defines a data broker as a "*company whose business is selling information about companies, markets, etc*.", we will use the definition of the US Federal Trade Commission [FTC12], which includes "*companies that collect information, including personal information about consumers, from a wide variety of sources for the purpose of reselling such information to their customers for various purposes, including verifying an individual's identity, differentiating records, marketing products, and preventing financial fraud*."

2.1.1 Existing data brokerage business models

An interesting fact about data brokerage comes from the data collection methods. A US Federal Trade Commission report on data brokerage [FTC2014] that included an in-depth study with nine data brokers finds that "none of the nine data brokers collect data directly from consumers." Instead, the report identifies three categories that correspond to the data sources about users, most of which are done without the knowledge of the users, namely (1) government sources, (2) other publicly available sources, and (3) commercial sources.

Figure 3 presents an overview of how the data from the sources pass to the information resellers (data brokers), which in turn sell them to the data users (typically businesses or government agencies) that need those data [GAO13]. "While each data broker source may provide only a few data elements about a consumer's activities, data brokers can put all of these data elements together to form a more detailed composite of the consumer's life." [FTC2014]

When it comes to the types of products offered by data brokers, the FTC report identifies three broad categories, namely (1) *marketing*, (2) *risk mitigation*, and (3) *people search* with an approximate revenue of $426 million in 2012 for the nine analyzed broker companies. An overview of the revenue distribution for these three main categories is provided in Figure 4.

As it can be seen and according to the FTC report [FTC2014], most of the revenue comes from data being used for *marketing* purposes, including "(1) direct marketing, which encompasses postal mail, telemarketing, and email marketing; (2) online marketing, which includes marketing to consumers on the Internet, on mobile devices, and through cable and satellite television; and

(3) marketing analytics.”

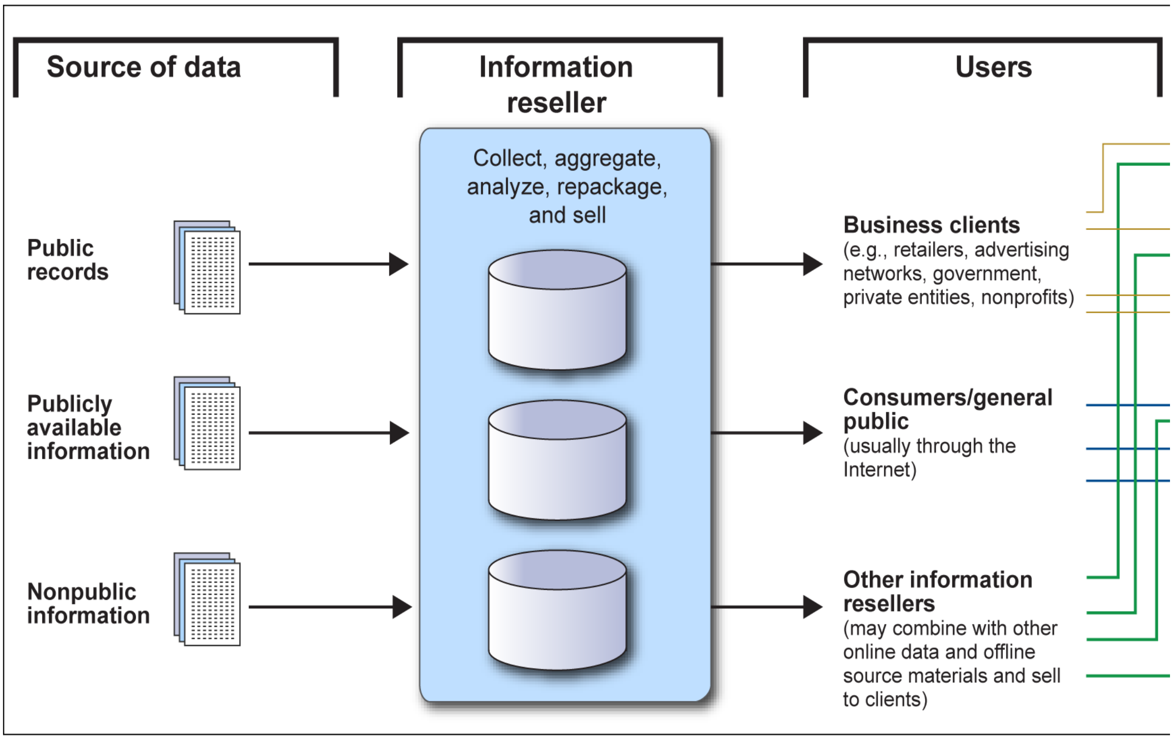
Source of data
Information reseller
Users
Collect, aggregate, analyze, repackage, and sell
Public records
Publicly available information
Nonpublic information
Business clients
(e.g., retailers, advertising networks, government, private entities, nonprofits)
Consumers/general public
(usually through the Internet)
Other information resellers
(may combine with other online data and offline source materials and sell to clients)

Figure 3. Typical flow of customer data through resellers to third party users - Adapted from [GAO13]

Next, risk mitigation products generate approximately $177 million for four of the given brokers. The report [FTC2014] identifies two main sub-products that are grouped into this category, namely (1) *identity verification* and (2) *fraud detection*. As described in the report [FTC2014], “identity verification products assist clients in confirming the identity of an individual. The data broker clients use identity verification products for diverse reasons. For example, banks use such products to comply with “know your customer” identity verification requirements under the USA PATRIOT Act[2] or to otherwise help deter fraud at the time a consumer commences a transaction.” Further, these services may take the form of a scoring format to assign different scores to transactions depending on their level of risk. In other cases, they may serve as an additional layer of authentication, typically including additional questions related to the user to confirm authenticity. Fraud detection, on the other hand, is used to help companies detect different kinds of suspicious or fraudulent transactions before they are finalized, such as wrong addresses, email addresses, and so on.

Finally, *people search* is the third category of revenues, which according to the report

[2] Customer Identification Programs for Banks, Savings Associations, Credit Unions, and Certain Non-Federally Regulated Banks, 31 C.F.R. § 1020.220 (implementing Section 326 of the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (“USA PATRIOT Act”), Pub. L. No. 107-56, 115 Stat. 272 (2001)).

[FTC2014] “provides personal information about consumers. These products may allow a user to conduct a search with as little as one data element, such as name, address, city/state, telephone number (including mobile telephone number), email address, username, or SSN” (Social Security Number) [FTC2014]. Furthermore, people search products are “unique in that they are often intended for use by individuals, although they can be used by organizations as well. Users utilize people search products for such purposes as tracking the activities of executives and competitors, finding old friends, researching a potential love interest or neighbour, networking, or locating court records” [FTC2014].

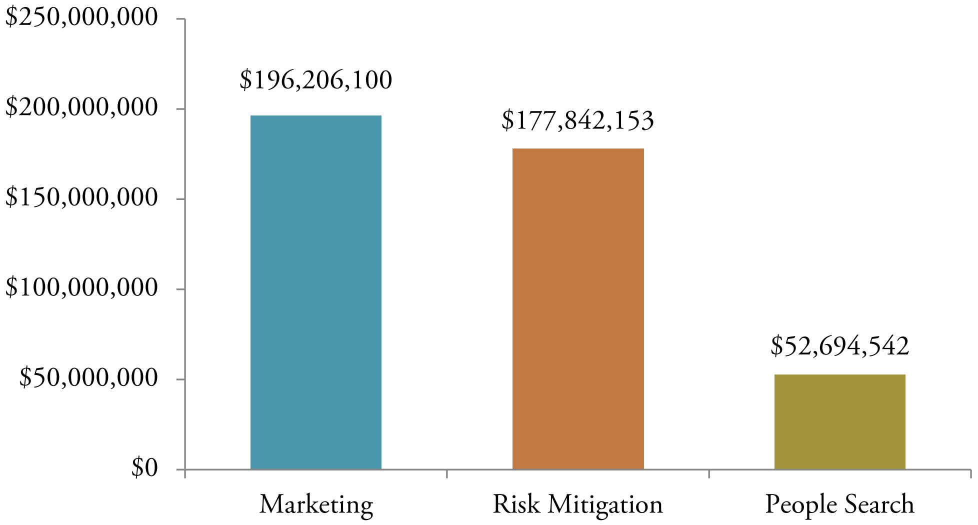

Figure 4. Revenues of nine Data Brokers by product category in 2012 [FTC14]

2.1.2 Data brokerage and Privacy-ABC technologies

As we saw earlier, data brokerage services are used in practice for a number of reasons. Furthermore, data brokers collect data about users from different sources and are dependent on these data sources both for the correctness and update of these data. As explained in the review of the data brokerage industry report [CCST13], brokers provide two types of data, namely actual data gathered directly about individuals, and modelled data, generated by inherence of different types of actual user data. In some cases, the sources may even provide fake data, especially if individuals have provided them with fake data in the first place (such as those coming from online polls or some loyalty programmes). Nevertheless, as noted in the FTC report [FTC14], data brokers offering identity verification services may have used such wrong inferences about individuals, which has resulted in wrongful denial of access to certain resources to users. On top of that, most of the data collection approaches are not transparent and are made without the awareness of the users.

Using Privacy-ABC technologies may be useful to address both of these issues. First, Privacy-ABCs are credentials that contain attributes that are certified by the Issuer. Using certified attributes would mean more accurate information about the users could be made available to the brokers and their clients. In turn, this would increase the effectiveness and accuracy of identity verification services provided by data brokers, such as for authentication. Second, using Privacy-ABCs in the right way has the potential to put users into control of the types of information they may be willing to share with data brokers. Furthermore, data brokers could provide some incentive for the users to disclose or correct certain amount of information held about them, which is already a practice among data brokers, such as the possibility to win a prize [CCST13].

However, one has to consider the extent to which Privacy-ABCs could be used to enhance privacy. While having certified attributes for cases where it is required and makes more sense would increase the assurance of the Verifier on the accuracy of the data, forcing users to always reveal certified data could work against the privacy of the users, as they would have less choice in giving away inaccurate data when they want to do so.[3]

However, the main point in this discussion is that the correct use of Privacy-ABC technologies would require less information disclosure by the users, enabling users to provide “blurred”, but useful information about them based on their credentials, such as, e.g. providing a proof that certain attribute value belongs in an certain interval rather than revealing the exact values. For instance, instead of showing the exact personal income, a user can confirm that her income lies within one of the pre-defined intervals, e.g. between 50,000-100,000 EUR per year. Privacy-ABCs support such a feature, namely doing predicates over attributes, in this case showing that the income attribute (assuming that the income is one of the attributes) is between 50,000 and 100,000 EUR without disclosing the attribute value.

As a conclusion of this discussion, the adoption of Privacy-ABC technologies in data brokerage practices could be useful for both users and data brokers. Users would gain more control and transparency about the types of data they would disclose to data brokers, respecting the principles of minimal and selective disclosure of personal data. While this can potentially reduce the amount of personal data gathered by data brokers, it can improve the quality of the data, since the data are usually certified. In addition, having the opportunity to provide the range of certain personal data rather than disclose the actual values, users may be more willing to disclose more information about personal data, giving both parties the desired benefits.

2.2 Personal Data Ecosystem Management

In the following sections, we will explain the concept of personal data ecosystem management, and describe the economic and privacy gains for the users. Specifically, an emphasis is given to the technical and business workings of the Respect Network as well as ways that Privacy-ABCs can be integrated into the Respect Network architecture.

2.2.1 Overview

In the new era of “anywhere, anytime” connectivity, more people connect to the Internet now in more different ways than ever before. The availability of pervasive connectivity has resulted in the collection of massive personal information by service providers. Not only does this massive collection of data harm the privacy of the users, but also deprives them of the economic benefits of their personal data that is recently being viewed as “the new oil of the Internet and the new currency of the digital world” [KUN09].

The success of the current business models of the digital economy depends on the how much personal data service providers can collect and on how many target persons they are able to profile. While this has raised the concern of privacy and economic benefits of personal data, the Personal Data Ecosystem (PDE) has emerged as a new landscape of companies and

[3] A similar point was also raised in one of the ABC4Trust Reference Group Meetings and is briefly described at Jaap-Henk Hoepman’s blog article: http://blog.xot.nl/2012/02/14/an-unexpected-privacy-risk-of-anonymous-credentials/.

organizations that believe individuals should control their personal data. One can think of personal data as the digital record of "everything a person makes and does online and in the world" [MMK10].

The compelling premises of the PDE is that individuals should be given the control and preference in sharing of their own data and set the rules as to who can access and use their personal information for what purposes. In this way the individual becomes the central point of data integration, and individuals always have the ability to extract their data and take it wherever they wish. PDE comprises three essential elements to function properly [CAV12]:

1. **Technology to control personal data:** this technical component includes the storage, access control, security, authentication, and user interface which provides the user with a set of features to manage their data and identity. The technology is designed in a way it facilitates the personal data ecosystem management. It is an element that goes among the users, service providers, and government laws.
2. **Supporting factors:** data management standards, communications standards, trust frameworks (rules and processes for the setting, monitoring and enforcement of permissions in permission-based information sharing), interoperability among various stakeholders and third parties, legal interoperability, regulatory requirements and settings. All of these supporting factors lay the foundation of a reliable and scalable PDE management.
3. **Stakeholders:** the main stakeholders in the emerging PDE are individuals who are increasingly managing and controlling their own personal data for their own purposes; specialist services such as Personal Data Vaults (PDVs) helping individuals to do this; governments and other public organizations; and private sector businesses that wish to begin sharing and using information with individuals on a new trust basis.

Currently the personal data is not fully exploited to the benefit of users due to "organization-centric" approaches in the management of personal data. Even though this approach is said to enhance user experience by using collected data and providing tailored services, it comes at the cost of lack of transparency and erosion of privacy. PDE stands in contrast with the "organization-centric" model used by Facebook, Google and others. While each of these online services collects, manages, and utilizes user data in a highly organized, systematic, professional and technologically advanced way to meet their organizational objectives, individuals have fallen behind in terms of having access to coordinated, advanced data management technology. The contemporary model is fragmented and inefficient for the following reasons:

- Users have limited control over the management and usage of their data;
- Each of the services has different privacy policies and settings;
- Users have little or no ability to manage privacy settings;
- Each online service requires users to establish a password and a user name, as well as to share detailed personal information (e.g. address, date of birth) specifically for that service, duplicating sensitive data and increasing exposure risk;
- Each online service must independently attempt to verify the online identity of the user to their required level of assurance; and,
- Each online service ends up with only a partial view of each user, leading to guesswork, error and waste.

Given the aforementioned drawbacks of the current business model, expectations surrounding what constitutes a healthy privacy-preserving relationship between individuals and organizations are being reset under the umbrella of PDE. PDE provides a "user-centric" model, which aims at unlocking such potential, by enabling individuals to control the gathering, management, use and sharing of data about them.

The value of personal data is quite subjective. Many business models have recently emerged that encourage and capitalize on the flow of that data. Recently, consumers are becoming increasingly aware of the value of the data they generate even in interactions like a trivial Google search. While direct personal data has an inherent value, secondary inferred data can also often be mined and interpreted to produce new information of equal or greater value. The long term impact of the aggregation and unchecked dissemination of this information is unknown.

In recent developments, innovative business model start-ups have emerged that entertain privacy-preserving personal data ecosystem management capabilities. Respect Network[4] is one such ecosystem that gives individuals the control over their personal data.

2.2.2 Respect Network (RN)

The Respect Network (RN) is a new paradigm business model that strives to empower people with their data. It is developed by the Respect Network Corporation, a PDE start-up supported by 16 founding partner companies around the world, including Neustar, an internationally-recognized neutral provider of real-time information and analysis, and Swisscom, Switzerland's leading telecom service provider which also has a good reputation of trust in Europe.

The Respect Network is conceived to be based on the principles of Privacy by Design. As such, privacy and personal empowerment are woven into the architecture of RN at the technical, legal and business model levels. The Respect Reputation System, as defined by the Respect Trust Framework, also gives all members of the network an immediate, strong, ongoing incentive to compete for their trust, not for personal data.

There is a general trend of increased migration to cloud solutions. The prediction is that cloud computing will grow even more as stated in Michael et al [MIC+10]. Therefore, RN gets its motivation of designing cloud based personal data ecosystem. It is designed to build personal cloud solutions that mostly user gets from Cloud Service Providers or in some cases from a personally owned cloud.

2.2.2.1 Business model

Respect Network provides a self-reinforcing business model, which stands for the benefit of the user and service provider. At the moment, there are individual users and Business member users, which provide services to individual users.

Respect Network's business approach comes with a number of significant advances as compared to existing business models involving personal data exchange. The advances include:

- Providing efficient business value exchange in which businesses pay only for what connections are worth to them.
- Permission based data exchange, which give customers the control of their own data.
- Member identity is verified.
- Individual members are incentivized to provide more and better data.
- The existence of a trust communication channel between businesses and customers.

Business members of the network pay for direct connections to their customers and prospects. Customers are also allowed to participate in the value created through these direct connections. To setup the connection, the Business cloud member pays a defined Relationship Fee. One third

[4] https://www.respectnetwork.com/

of the fee goes to the benefit of the customer. As such, the user does an informed decision as to who accesses her data as well as substantial economic benefit.

2.2.2.2 Respect Connect as replacement to social login

Social login sign-on services available from social networks like Facebook, Twitter, LinkedIn, and Google have become the most widely adopted form of federated identity on the Web. The wide acceptance of social logins is due to the advantages they provide to users and relying parties. From user side, social logins reduce sign-on friction and foster ease of use of accessing services. At the same time, from the relying parties point of view, social logins provide the provision of reduced sign-on friction, ease of development, and the capability to leverage personal data.

Despite the relative advantages they provide, social logins do however introduce a middleman into the online relationships that not all individuals and relying parties are comfortable with. Users raise deep privacy concerns for their real personal information is exposed to all the social network's partners involved in the process of authentication. Often there is lack of control of what is happening, which eventually builds in independency on third party.

Relying parties also raise the concern of having a third party in the middle of customer relationships. Besides making relaying parties dependent on third parties, social logins damage the trust of users to the relaying party. In addition, the relationship is subject to facing a risk of changing terms and costs over time.

The emergence of personal clouds is setting the stage for a new type of federated login that will work directly from personal clouds, positioning the individual as a peer on the network with enhanced privacy, greater control and no middleman intruding into customer relationships with relying parties.

Personal cloud login sign-on services such as Respect Connect provide users the possibility to access website or application through their personal clouds. As such, Respect Connect stands as viable replacement for social login sign-on for the following benefits it provides:

- Reduced sign-on friction (users and RPs)
- Increased trust (users and RPs)
- Safe data sharing in either direction (users and RPs)
- Lifetime data subscriptions (users and RPs)
- Cloud service providers gain market share, leverage and new revenue streams

The personal cloud login sign-on through Respect Connect uses the XDI (eXtensible Data Interchange) protocol to establish the communication channels. Channels may pass any type of message between personal clouds, not just text, images, and attachments. Messages may include event notifications, data queries, and data transfers. XDI helps create 'link contracts' i.e. it provides built-in authorization for the contractual relationship between the business and personal clouds. It is designed on the idea of 'link contracts' that define security and privacy requirements that must be adhered to when handling the data referred to by the link contract.

2.2.2.3 Integration of Privacy-ABCs into the Respect Network

There are different ways how Privacy-ABCs can come into the architecture of Respect Network. Respect Network provides users with Respect Connect personal cloud sign-on as a replacement of social logins.

Currently, Respect Connect sign-on is being designed to use either OAuth or XDI signed messages for authentication. The former is more widely used; the latter is more secure.

Therefore, for communication with other service providers Respect Connect is utilizing OAuth due to wider usage of OAuth. When a user triggers the Respect Connect personal cloud login from websites, the client software opens a channel with their personal cloud. The personal cloud then acts on behalf of the user to communicate with the service provider that the user wants to have access to. Essentially, the personal cloud opens an OAuth authorization process with the service provider on behalf of the client when the client requests authorization from the resource owner. The authorization request, in this case, is made indirectly via the personal cloud as an intermediary.

After successful authorization, the client receives an authorization grant which is a credential representing the resource owner's authorization. The client will also be provided with an access token, which in turn, is used to access the protected resource.

In this authorization process that takes place between the personal cloud and the service provider, Privacy-ABC technologies can be exploited in such a way that they improve the privacy gains of users because they provide the following features as stated in the architecture deliverable of ABC4Trust [BIC+14]:

- Privacy-ABCs are by default untraceable, service providers are not able to track and trace the usage of the users' information.
- Privacy-ABCs enable users to authenticate under pseudonyms.
- Privacy-ABCs allow users to have access to resources with minimalistic information disclosure.
- Privacy-ABCs provide high security using asymmetric cryptography.

In the authorization communication that happens between the personal cloud and the business member of the network, the personal cloud can be designed to acts as ABC-agent mediating the user and the service provider.

A successful authorization process grants the user with an access token. Therefore, it is also possible to create and define Privacy-ABC access tokens. Likewise, it is also possible to embed the ABC access token messages into the multiple access token request-response OAuth messages thereby replacing potentially personally identifiable information. This is possible because the current specification of OAuth format and contents of the access token is not defined in the OAuth specification [BIC+14], hence one could define a way to use a Privacy-ABCs to create an access token.

3. Privacy-ABC technologies and new business models

Besides the potential for integrating into existing data-brokerage models, the adoption of Privacy-ABC technologies could also provide a potential for new business models. In the first section in this chapter we discuss business models around providing Privacy-ABC features as services. In the second section, we consider the domain of online advertisement, and discuss the possibility of integrating Privacy-ABC technologies to provide a new paradigm of privacy-enhancing advertisement.

3.1 Privacy-ABC features as services

The architecture of Privacy-ABC technologies [BIC+14] recognizes two core processes, issuance and presentation, as well as two optional processes, inspection and revocation. Each of these processes can be considered as features of Privacy-ABCs, which is provided by a particular entity within the system, e.g. issuance is provided by the Issuer, whereas different Verifiers take charge of verification of presentation tokens. Providing each of these services requires implementation and running of respective entity components, e.g. an Issuer, a Verifier, an Inspector, or a Revocation Authority.

In an isolated architecture, one could naturally implement and run all of these services at one's premises. However, the architecture and its elements could be deployed for a wide number of applications and scenarios. Considering the prominence and deployment advantages of cloud-based services, this business model could be seen as a subcategory of infrastructure-as-a-service model in the cloud.

It could be that a bank or some other trusted entity, be it public or private, runs an eID infrastructure based on Privacy-ABC technologies and could serve as an Issuer of Privacy-ABCs for its users. These credentials could then be accepted and used also outside of the bank, such as for age verification, authentication into different portals, and so on. Each of these services that accept Privacy-ABCs would need to run a Verifier that would check the validity of the presentation tokens received by the users. However, as having verification supported internally would require that the service providers would implement and maintain the necessary Verifier components, which may be costly and complex. For this purpose, there could be that some external entity could provide *Verification as a Service* similar to the cloud-based services to other companies who may natively rely on other technologies and choose to outsource the implementation and running of a Verifier. The benefit for service providers would also be similar to the benefit of using the cloud: the services are outsourced to a specialised company, shifting the responsibility to them and lowering the cost for maintaining it. In this case, such a service would then translate different security policies into ABC4Trust-compatible presentation policies and provide the possibility to verify user's presentation tokens on behalf of these service providers.

However, although service providers could choose between different such external providers of verification services, it must be understood that such a deployment model tends to put the entity that provides verification as a service into a stronger position, as more presentation sessions would go through them. As a result, depending on how different presentation policies are defined (depending how much linkability is provided by different presentation policies about the users, e.g. depending on the fact on whether or not attribute values are disclosed and the types of such attributes), the entity providing verification as a service could potentially learn more about the users by combining information from presentation policies of different service providers that outsource this service to them. This approach could nevertheless prove useful for further adoption of Privacy-ABC technologies, and provide an additional layer for interoperability with other technologies. The business model could vary, from per-transaction fees to monthly or yearly flat rates for such services, with the service providers paying for the services to the entity that provides them with the capability of verification as a service.

Besides verification, with a potential adoption of Privacy-ABC technologies, one could certainly serve other functions as well, such as *Revocation as a service* for one or more Issuers and provide the revocation service to a number of such Verifiers. In the ABC4Trust architecture, the job of the Revocation Authority would be to maintain the list of revoked credentials and inform the other entities (Verifiers) either automatically or on demand about the status of this list. Hence, besides revoking credentials, an important part of the responsibility of this entity is the dissemination of revocation information to Verifiers and Users. An Issuer-driven revocation would still require that the revocation request would be initiated and authorized by the Issuer of Privacy-ABCs, so the power to decide on revocation would still be at the Issuer. The revenue model for providing such a service could vary, but one could think of e.g. charging the Verifier a fixed fee for each update on the latest revocation information, or providing "flat-tariff" for a certain monthly or yearly rate. Depending on the revocation model chosen, this service could be provided both as an Issuer-driven and a Verifier-driven type of revocation, but the business model for both may vary, as would the efforts to provide such a service.

Following a similar model, besides verification and revocation, one could provide *Inspection as a Service*. Technically, inspection provides accountability for otherwise unlinkable and pseudonymous transactions of the users. As one would need to provide the service constantly and efficiently, this may involve not only technical, but also legal requirements in order to assess the right model of inspection for different scenarios. Overall, offering inspection as a service could follow a similar business model to the previously described proposal for revocation as a service. In addition, running such a service requires a particular level of trust by all parties, especially by Verifiers and Users. If implemented by an independent entity with a good reputation, it might as well increase the trust level into Privacy-ABC technologies and the applications that are using them. Furthermore, the service of an inspector could be distributed between different Inspectors, who provide inspection services for their clients. If desired, the user can be given the choice of the inspector authority, giving an additional layer of transparency and choice, as well as providing competition in the market.

3.2 Privacy-enhanced advertisement

Online advertising is a powerful driver and force in todays Internet economy. Many "free-services" on the Internet are provided to users in exchange for their personal data, allowing personalised services. Typical practices used for providing personalised advertisement include, but are not limited to, online behaviour tracking, collection and processing of personally identifying information, and using detailed profiling techniques.

While advertisers want more information about users to provide targeted ads, users demand more privacy and oppose to existing tracking approaches [HUL12]. In this context, the privacy of the users does not necessarily mean no advertisement or no tracking, but rather being in control to define their policies and have advertisers respect their choice on the type of tracking and advertisement.

Privacy advocates have raised issues about the tracking of online user behaviour, and some have even deployed alternative tools to provide ads whilst respecting the privacy of the users, such as the Privad framework [PRIVAD] by Max Planck Institute for Software Systems, which serves as a browser add-on and hides the internet address of the users from the advertisers.

Furthermore, the European Project PICOS has created a prototype, which provides a component for privacy-preserving advertisement for social networks [KC+11]. It was meant to serve the multilateral interests of all the involved stakeholders in chosen communities. For the users, it provides an opportunity to hide certain information from advertisers, such as location blurring, and use different partial identities for different contexts. This concept is quite similar to the Privacy-ABCs[5] and could be used to provide such targeted and viral advertising to users by adhering to their individual choices of privacy policies, which follow intuitively the concept of the user control promoted by Privacy-ABCs.

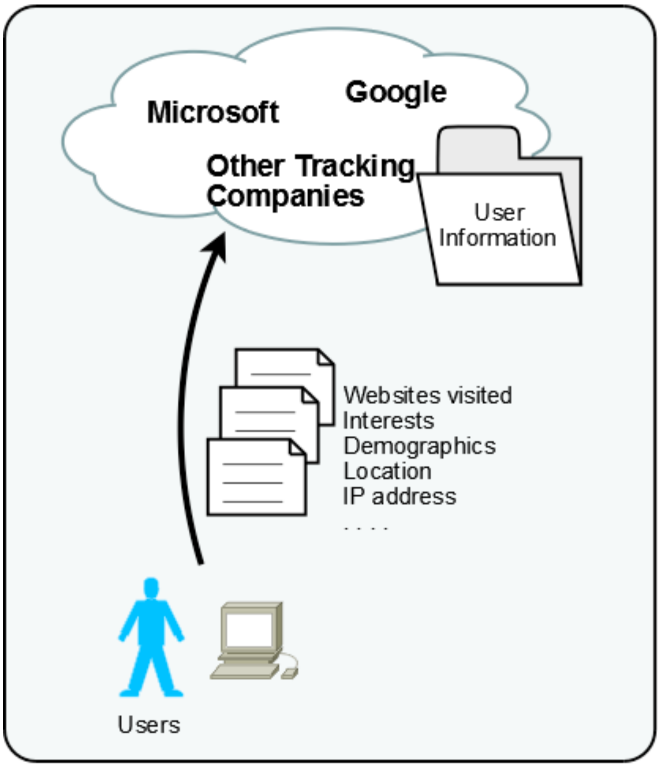

Figure 5. Current model of tracking user's online behaviour for advertising [RPIA]

Furthermore, advertisers may not always need all the precise information about users in order to provide them with personalised advertisement, such as income, birthdate, address, and so on. Instead, they may provide similar targeted ads by having categorised information about users, such as age range or income range, as well as the area where the user lives. This is perfectly possible by using features of Privacy-ABCs, such as predicates over attributes to show that the user is of a certain age range, and similar for income or place of living.

[5] Indeed, the concept itself goes in the same direction of more privacy for the users. However, PICOS aimed at testing the usability and understanding of the promised features by the users. It did not implement the privacy-preserving components that are used in ABC4Trust, but rather required trust on the platform where the service was running with the promise that certain features would be properly handled at the application level rather than by architecture design, contrary to what ABC4Trust provides.

Being in control on the type of information that they give away for advertising purposes will empower users and may motivate them to reveal additional parts of their identity information to the degree chosen by the user. In addition, this will improve the quality of the information that advertisers would be dealing with, since Privacy-ABCs contained certified attributes (identity information) about users, leading to a potentially more qualified advertisement.

The concrete business model for such a privacy-enhanced personalised advertisement scheme would depend on a number of factors. First and most important, one has to consider the source of the personal data. While some of the data used for advertisement are collected through data brokers, others may be collected directly by the companies that operate the services that collect the data, such as Amazon or E-Bay. In the former case, the business model for the advertisers would not be affected, whereas the latter could provide additional business benefits for the Users: the service provider could encourage users to share certain information from their credentials solely for advertising purposes by giving them direct benefits. This can be direct financial compensation for the data, or discounts and vouchers for providing certified data from the users.

4. Conclusion

Privacy-ABC technologies are an important building block of identity management systems that respect both the interests of the users and of the service providers. Due to their innovative architecture and user-centred design, its adoption have the potential to influence a number of existing business models, especially those that have a stronger relation to the personal data about individuals. In this report, we have a number of concrete business examples and assessed the potential impact the adoption of Privacy-ABC technologies would have in their business models. We recognize that Privacy-ABC technologies provide additional benefits not only to users, but can also improve the quality of service in the identified cases, resulting in benefits also for the service providers.

Despite the potential minimisation of the data that would be collected by these service providers, the increase in the quality of the data collected, as well as the potential for more privacy-respecting data collection and processing can make up for this. Providing more transparency to the users and giving them more control about their personal data disclosure may even motivate users to share some types of information, even if these data are less personally-identifying. This could in turn improve the quality of the services for data brokers, as they would be working with more quality data.

Further, we also showed that Privacy-ABC technologies could be integrated with new and innovative business model, namely Respect Network, which promotes a new paradigm with a self-reinforcing business model aiming at empowering users through their personal data. It is both beneficial and feasible to integrate Privacy-ABC technologies into the architecture of Respect Network.

In addition to impacting existing business models, Privacy-ABC technologies also have the potential to drive new business models, especially in providing some of the features of Privacy-ABCs as services, providing similar service and benefits as the Infrastructure-as-a-Service in the cloud. Typical such services that could be outsourced include verification, inspection, and revocation. Each of these features may have its own specific requirements based on the application area where they serve, but the potential to provide such services exist.

In addition, we provide some insights on the potential of using Privacy-ABC technologies could promote and enable a new form of personalised advertisement, which respects the privacy of the users. Putting the user in control could create a business model that gives the user also more power not only in deciding which information to disclose, but also negotiating direct benefits for them, both financially or through vouchers in exchange for providing certain information about them. And the best of all is that these personal data can be randomized so that they become less identifying, but are still useful for the advertisers.

Needless to say, the list of new business models is not comprehensive, but is also not meant to be. Rather, we want to show that Privacy-ABC technologies not only provide useful features for the users, but they may also enable new business models, which can also be an additional driver for the adoption of these technologies.

5. References

[ACQ10] A. Acquisti. "The Economics of Personal Data and the Economics of Privacy". Background Paper for OECD Joint WPISP-WPIE Roundtable 1 2010.

[BIC+14] P. Bichsel et al. D2.2 Architecture for Attribute-based Credential Technologies – Final Version, 2014.

[CAV12] A. Cavoukian. Privacy by design and the emerging personal data ecosystem. Privacy By Design, 2012.

[CAV13] A. Cavoukian. Personal Data Ecosystem (PDE) – A Privacy by Design Approach to an Individual's Pursuit of Radical Control. Digital Enlightenment Yearbook 2013: The Value of Personal Data, 2013.

[CCST13] United States Senate - Committee on Commerce, Science, and Transportation. A Review of the Data Broker Industry: Collection, Use, and Sale of Consumer Data for Marketing Purposes. Staff Report for Chairman Rockerfeller, 2013.

[FTC12] Federal Trade Commission. Protecting Consumer Privacy in an Era of Rapid Change, March 2012.

[FTC14] US Federal Trade Commission. Data Brokers - A Call for Transparency and Accountability, May 2014.

[GAO13] United States Government Accountability Office. Information Resellers - Consumer Privacy Framework Needs to Reflect Changes in Technology and the Marketplace. Report to the Chairman, Committee on Commerce, Science, and Transportation, U.S. Senate GAO-13-663, September 2013.

[HUL12] C. J. Hoofnagle, J. M. Urban, S. Li. Privacy and Modern Advertising: Most US Internet Users Want "Do Not Track" to Stop Collection of Data About their Online Activities, Amsterdam Privacy Conference, 2012. Available at: http://ssrn.com/abstract=2152135.

[KC+11] C. Kahl, S. Crane, M. Tschersich, K. Rannenberg. Privacy Respecting Targeted Advertising for Social Networks. In IFIP WISTP 2011, pp. 361–370, 2011.

[KUN09] M. Kuneva, European Consumer Commissioner, “Personal data is the new oil of the Internet and new currency of the digital world.”, March 2009.

[MIC+10] A. Michael *et al*. "A view of cloud computing." *Communications of the ACM* 53.4: 50-58, 2010.

[MMK10] D. Marc, R. Martinez and C. Kalaboukis. “Rethinking Personal Information – Workshop Pre-read.” Invention Arts and World Economic Forum, 2010.

[MM12] C. Moiso, R. Minerva. “Towards a User-Centric Personal Data Ecosystem,” Paper presented at the 16th International Conference on Intelligence in Next Generation Networks, Berlin, Germany, 2012.

[PRIVAD] S. Guha, B. Cheng, P. Francis. Privad: Practical Privacy in Online Advertising. Available at https://adresearch.mpi-sws.org/privad-nsdi.pdf.

[RPIA] Max Planck Institute for Software Systems. Research on Privacy in Internet Advertising. Available at https://adresearch.mpi-sws.org/overview.html.