5-15-2019

UNDERSTANDING PREPROTOTYPE USER ACCEPTANCE OF CENTRALISED AND DECENTRALISED IDENTITY MANAGEMENT SYSTEMS

Johana Cabinakova
Goethe University, johana.cabinakova@gmail.com

Nadine Kathrin Ostern
Frankfurt School of Finance & Management, n.ostern@fs.de

Julia Krönung
University of Mannheim, kroenung@bwl.uni-mannheim.de

UNDERSTANDING PREPROTOTYPE USER ACCEPTANCE OF CENTRALISED AND DECENTRALISED IDENTITY MANAGEMENT SYSTEMS

Research paper

Johana Cabinakova, Goethe University Frankfurt, Frankfurt, Germany, johana.cabinakova@stud.uni-frankfurt.de

Nadine Kathrin Ostern, Frankfurt School of Finance & Management, Frankfurt, Germany, n.ostern@fs.de

Julia Krönung, Mannheim University, Mannheim, Germany, kroenung@bwl.unimannheim.de

Abstract

Decentralized identity management systems (DIMS) open up new opportunities for identity management, meaning that decentralization and the lack of a central party are expected to provide users' of DIMS with more control and transparency over their personal information. Thereby, DIMS are in contrast to traditionally used centralized identity management systems (CIMS) that are, nowadays, often realized by the implementation of so-called SSO schemes, which allow users to authenticate once with a particular service provider and to use these credential for every subsequent authentication. In the literature, control over personal information is often hypothesized to affect information self-disclosure; however, only little is known on how control affects disclosure behaviour depending on the design of IMS user interfaces. We show through a multi-group structural equation analysis that perceived control is a stronger predictor on user disclosure behaviour in the DIMS environment compared to the CIMS. Furthermore, the results of our study provide practical implications on user interface design based on the effect that perceived ease of use of interface does not necessarily enhance user attitudes towards the IMS.

Keywords: Preprototype Testing, Identity Management Systems, Blockchain, Technology Acceptance.

1 Introduction

An average online consumer has no less than 90 online accounts (Dashlane 2015). To receive specific news or to stay up to date with the latest sports results, to buy a cinema ticket, to use the favourite music or video streaming provider, to make the yearly tax declaration online or to organize an appointment by ones' general practitioner: Online users are obligated to reveal information about themselves that make them uniquely identifiable for using a particular service. The digital representation of information about an individual, called *digital identity* (Squicciarini et al., 2006), is as important as every other precious and sensitive document we own in today's world. However, while we can capture our passports, health cards or social security number safe in our houses, we struggle to do so in the online world, especially when it comes to information that makes us identifiable.

How digital identities are managed is lagging in functionality to the requirements of the technological advancements of present times. Managing the resulting identities in online environments manually is, principally, feasible. However, it is a tedious task defying the surplus value of speed and convenience provided by only transactions and processes. To maintain surplus value, identity management systems (IMS) provide automated solutions for managing roles and identities that are either determined by the respective support of the administration of information subjects or support active management of personal information (Hansen et al., 2004; Zwattendorfer et al., 2011). A recent and prominent example of a centralized IMS (CIMS) is a single-sign on (SSO) scheme, which allows users to identify and authenticate once and to gain access to different resources in a distributed computing environment (Zwattendorfer et al., 2011). While nowadays SSOs are provided by nearly every leading web company (e.g., Facebook or Google), they deprive online users of the control and transparency over revealed information and expose them to significant risks (i.e., identity theft, data abuse). This is because data that are provided by users to authenticate using the SSO are stored in a centralized fashion, which provides a point of attack for hackers. Notably, we are aware of the fact that various proposals exist to increase SSOs' security by implementing control mechanism and that these mechanisms are partially already available in the form of software standards, libraries, and implementations (Hansen et al., 2004). However, their practical application is still a problem, and the concrete goals of user anonymity and unlinkability are usually not achieved perfectly (Hansen et al., 2004; Clauß et al., 2005).

As a consequence, IMSs have developed from being organization-centric to user-centric, meaning that CIMS are replaced by solutions, where users' themselves store identifiers and credentials from different services in a single tamper-resistant hardware device or software (Jøsang and Pope, 2005). To put users back at the centre of the identity management process, the concept of CIMS was recently challenged by blockchain-based, decentralized identity management systems (DIMS). These systems intend to eliminate the necessity of third-parties and enable users to take ownership over their personal information and data, increase data transparency as well as fine-grained access control (Zyskind et al. 2015). Currently, there are only a few authoritative reports and whitepapers avialable, that inform concisely about DIMS functionalities and present their philosophy on the matter (Table 1).

As to the authors best knowledge, hitherto, there exists no studies that examines how users' attitudes toward CIMS and DIMS differ, when it comes to their perceptions of control and transparency as well as the associated willingness to disclose personal data. The fact that there exist no such studies is surprising, as the failure rate for newly developed information systems remains unacceptably high, especially for large and complex systems (Davis and Venkates, 2004) as DIMS are. A part of the problem is that it is conventional wisdom among system developers that prospective users must have hands-on experience with at least a working prototype of a new system to provide an assessment that accurately reflects future user behavior. However, a study conducted by Davis and Venkatesh (2004) reveals, that it is highly beneficial to predict the acceptance of a new system based on users' evaluation captured during the earliest stages of the development of an information system, ideally before building a working prototype (Davis and Venkatesh, 2004). Following the timeline of the *preprototype user acceptance testing* (Davis and Venkatesh, 2004), we argue, that whitepapers propsing DIMSs are currently at a point in time, where sufficient information is available to describe the design of a DIMS

to potential users. In particular, this holds, even if the details of specific commands, menus, screen, and data elements have not been specified yet (Davis and Venkatesh, 2004).

Thus, instead of comparing SSO schemes to centralized approaches of identity management with incremental advancements concerning control and transparency over users online identity, this study compares the entirely new approach of DIMS to CIMS. In this regard, the objectives of the study are to elaborate on the concept of DIMS and CIMS and to examine their effects on users' self- presentation behavior.

The remainder is structured as follows: The subsequent section is concerned with the conceptualizations of CIMSs and DIMS as well as its functionalities and characteristics regarding the factors control and transparency. Subsquently, the research model together with the hypotheses is presented. Section 3 presents information about methodology and study results. A multi-group analysis is performed that allows identifying the difference between users attitudes toward CIMS and DIMS. In section 4, these results are discussed and classified in the context of the existing literature. Finally, a conclusion and outlook is provided.

2 Conceptualization of Identity Management Systems

2.1 Centralized Identity Management Using Single-Sign On Schemes

As a result of strategic self-presentation and information disclosure, individuals tend to have numerous partial identities in the online world (i.e., partial identities for private or professional social networking). Associated with the increasing number of partial identities is the rapidily growing need for automated solutions for managing roles and partial identities in various online contexts. Using identity management systems (IMS), which help individuals to manage their online accounts and partial identities, are, thus, nowadays a common practice (Scott et al., 2017). IMSs are responsible for the fail-safed assignment of attributes to an individual, for the sake of online authentication and to reach liability (Clauß et al., 2005). With the boom of online service and social networking in recent years, web-based single sign-on (SSO) schemes are increasingly deployed. The benefits of this kind of IMSs is that users of SSO schemes only need to authenticate once by using a credential. Afterwards, the user has access to multiple resources and applications within a distributed computing environment without the need to authenticate a second time (Suriadi et al., 2009; Zwattendorfer et al., 2011; Wang et al., 2012).

During the authentication process of an SSO, a user submits his or her credential (e.g., a user ID, a password, or the result of a cryptographic operation, involving his or her credential) to the authentication authority. Depending on the credential, the user can either remember the credential or store it on devices like a smart card. In the next step, the authentication authority validates the credential using data stored on its credential database (e.g., LDAP). If the information submitted through the user matches the data on the database, the user's identity is considered as authentic, i.e., a user receives access to a particular online service. To proof that the user has been authenticated, the authenticating authority issues a token to the user. This token is used as a proof of authentication for subsequent access to the service (He, 2000; Clercq, 2002).

Using the SSO leads to benefits on the user side: First, users do not need to log in each time they want to access a service. Second, in case that credentials need to be changed, users must alter only one set of credentials instead of each credential for each service that is used. These key advantages are a result of the fact that data are stored centralized, meaning that data access and manipulation may happen using the same tools and procedures (Clercq, 2002; Pashalidis and Mitchell, 2003). However, while in theory, the use of a centralized authentication approach seems favorable, because of the convenience of use, data centrality implied by SSO schemes is also a key vulnerability within the authentication process (Clercq, 2002). Scott et al. (2017) identified several threats and vulnerabilities to SSO schemes, including phishing attacks, attacks that are targeted on the applied login standard (e.g., OpenID or OAuth) as well as further web-based vulnerabilities.

2.2 Control and Transparency through Decentralized Identity Management

The technological backbone to realize decentralized identity management systems (DIMS) is blockchain (Fromknecht and Velicanu, 2014; Zyskind et al., 2015; Shrier et al., 2016). Nakamoto (2008) initially proposed the technology in the context of the decentralized e-payment system Bitcoin. Blockchain combines cryptographic techniques and decentralized consensus mechanisms to create publicly verified records, which consist of storage units (so-called blocks), which are linked together (Narayanan et al., 2016). Despite there exist various proposals how to apply the technology for DIMSs (Table 1), we focus on the work of Zyskind et al. (2015), providing the most precise description of a DIMS hitherto.

Name	Excerpt of the official description	Source
Selfkey Key	„... blockchain based self-sovereign identity system.“	SelfKey Whitepaper (2017)
DiroToken	„... fully decentralised and reliable global identity plat-	Diro Whitepaper (2018)
AuthenticID	„... providing the optimal level of proven identity authenti-	AuthenticID Whitepaper
Cove Identity	„…robust, multi-faceted digital [identity] verification	The Cove Whitepaper (2017)
BotChain	„…verify bot identity.”	BotChain Whitepaper (2017)
Civic	„…verified identity decentralized with blockchain tech-	Civic Whitepaper (2018)
Honestis Net-	„... keep your digital identity well managed […] decentral-	Honestis Whitepaper (2017)
VerifyUnion	„... Digital Identification […] without […] centralized	VerifyUnion Whitepaper
Nuggets	„… an ID platform […] stores […]data […] in the	Nuggets Whitepaper (2017)

Table 1. List of whitepapers describing a DIMS

Zyskind et al. (2015) describe a blockchain based DIMS, wherein the blockchain takes the role of mediator between users, services, and service provider respectively. They note that, while users of DIMS usually remain (pseudo)anonymous, storage of service profiles on the blockchain is generally applicable and so is the verification of their identity. Applied as the backbone for the DIMS, the blockchain accepts two types of transactions: T_{access}, used for access control management and T_{data}, used for data storage and retrieval (Zyskind et al. (2015).

The following example shows how the DIMS works in detail: A user installs a DIMS application on his or her computer or any other device with Internet connectivity. As the user signs up for the first time, the DIMS generates a new shared (user, service) identity and sends it to the blockchain using T_{access}s transaction along with the associated permissions. Data that is collected through the application is then encrypted by a shared encryption key and sent to the blockchain using T_{data} transaction. Subsequently, encrypted data is routed to an off-blockchain key-value store, while retaining only a pointer to the data on the public ledger (Zyskind et al. 2015). Both, the service and the user can now query the data using a T_{data} transaction with the pointer (key) associated with it. Using the blockchain, the DIMS then verifies whether or not the digital signature belongs to either the user or the service (Zyskind et al. 2015). Permission of the service to access the data is checked as well. Finally, the user can change permissions granted to a service at any time by issuing a T_{access} transaction with a new set of permissions, including revoking access to previously stored data (Zyskind et al. 2015).

Hence, using DIMS, only users have control over data (Zyskind et al. 2015). The decentralized nature of the blockchain combined with digitally-signed transactions ensures that an attacker cannot pretend to be a user, or corrupt the network, by gaining control over the majority of the network's resources (e.g., computing power) (Zyskind et al. 2015). More than that, DIMSs provide users complete transparency over what and how many data is collected about him and by whom they are accessed (Zyskind et al. 2015). Overall, the blockchain-based DIMS presented by Zyskind et al. (2015) provides users with more and, in particular, with more flexible control over permission rights than a CIMS. In contrast to the majority of SSO schemes, which require full permission to access data already during the initial sign-on, DIMSs enable fine-grained access control.

2.3 Research Model and Hypotheses

To examine how users perceive and evaluate CIMS and DIMS, we developed a research model, which is illustrated in Figure 1. The construct attitude represents the core variable of our research model and is defined as *"a psychological tendency that is expressed by evaluating a particular entity with some degree of favor or disfavor"* (Eagly and Chaiken, 1993, p.1). Previous findings show that attitude is a good predictor of users' behavior (Davis et al., 1989). Thus we expect attitude to capture users' perception of CIMS or DIMS, helping us to make reliable predictions about users' behavior concerning the IMSs.

To explore factors that impact users' attitudes either towards a CIMS (i.e., a SSO scheme) or DIMS, we apply the frequently used constructs *perceived usefulness* and *perceived ease of use* that originally stem from the technology acceptance model (TAM) (Davis 1985, 1989). Notably, both constructs are expected to affect individual's attitude towards the respective IMS, whereas a positive attitude is a strong predictor of the intention to use an IMS (Davis, 1985; Venkatesh et al., 2003).

If systems are easy to use, less effort by the user is required, which increases the likelihood of their use (Davis et al. 1989). We expect that users' perception of the *ease of use* of the SSO scheme is lower than in case of using a DIMS, since the SSO requires the user to remember his or her account access information every time he or she wants to authenticate (Khattak et al. 2011). In contrast, using a DIMS, personal information is owned by the user and stored encrypted on a separated device (e.g., smart phone, tablet). The user does not need to remember this information. Therefore, we hypothesize:

H1. *For users of DIMS, perceived ease of use is a stronger predictor of attitude towards an IMS than for users of CIMS.*

With respect to the users' perceived usefulness, we expect perceived usefulness of the DIMS to be a weaker predictor for attitude towards the IMS, which can be reduced to the fact that the user interface of the DIMS compared with the user interface of the SSO scheme provides much more decisional freedom, i.e., users can make more decisions on which information is shared with whom. Thus, DIMS imply a degree of complexity that goes beyond mere accept/non-accept-decisions that prevail in the SSO scheme. Therefore, we hypothesize:

H2. *For users of DIMS, perceived usefulness is a weaker predictor of attitude towards an IMS than for users of CIMS.*

TAM posits that perceived usefulness will be influenced by perceived ease of use because, other things being equal, the easier a system is to use, the more useful it can be (Venkatesh 2000). In the context of IMSs, perceived ease of use should influence perceived usefulness directly, because when users perceive its use easy, they will be more likely to use the IMS. Individuals' perceptions of the usefulness of a technology are determined to a great extent by the technology's perceived characteristics and attributes, whereby, these attributes, in turn, depend on the user's perceived complexity of an IMS or, in other words, on its ease of use (Moore and Benbasat, 1991; Rogers, 1995). We hence expect that the benefits that arise from data ownership in the DIMS outweigh the hypothesised negative influence of perceived usefulness of the DIMS. Consequently, we expect:

H3. *For users of DIMS, perceived ease of use is a stronger predictor of perceived usefulness of the IMS than for users of CIMS.*

Several studies have emphasized the role of perceived control on peoples' voluntary self- disclosure behaviour in divergent contexts, such as e-commerce or online social networks (Malhotra et al., 2004; Acquisti and Gross, 2006; Dinev and Hart, 2006; Taddei and Contena, 2013). In particular, if people perceive themselves as less able to control information and protect themselves, they are less disposed to disclose information about themselves (Weber, 2009; Taddei and Contena, 2013). Vice versa, if people perceive higher control, they are likely to disclose more data, for instance, if users are enabled to limit the access to personal information stored on an online account by setting fine granular privacy settings (Weber, 2009; Krasnova et al., 2010). Since DIMSs provide substantially more control over data than conventional SSO schemes, we expect that users of DIMSs disclose more information voluntarily than users of the SSO scheme. In particular, users of the DIMS can decide which and how

many information is shared with, for example, an online service provider and thus, this raises the perception of users to interact in a more secure environment (Benford et al., 2006) than using the SSO scheme, which fosters self-presentation and self-disclosure.

Moreover, to decide which and how many information is voluntary disclosed, users of IMSs must know what and how many information is required. We assume that using a DIMS, transparency over self-disclosed data are a direct consequence of the control mechanisms applied. Thus users of the DIMS are expected to perceive higher transparency over self-disclosed data that are revealed using the present control mechanism. Given the fact that the control mechanism using SSO schemes are limited, users' perceived transparency is expected to be lower (Benford et al., 2006; Krasnova et al., 2009).

H4. *For users of DIMS, perceived control of self-disclosed data online is a stronger predictor of willingness to self-disclose data than for users of CIMS.*

H5. *For users of DIMS, perceived control of self-disclosed data online is a stronger predictor of perceived transparency of self-disclose data online than for users of CIMS.*

Eventually, users that have a perception of control and transparency within an information system are more likely to have a positive attitude towards the respective system, since transparency gives users the information necessary to make a judgment on the respective IMS (Nicolaou and McKnight, 2006). We expect that users' judgment is better referring to the DIMS since it provides reasonable more information and control on personal data and data use that the SSO scheme. Thus, we hypothesize:

H6. *For users of DIMS, perceived control of self-disclosed data online is a stronger predictor of attitude towards the IMS than for users of CIMS.*

An effect of the hypothesized perception of control in the DIMS due to, e.g., the possibility to set fine-granular privacy settings in online social networks or in e-commerce relationships, is that users must be informed about protection and control mechanisms and their functioning. This provides users with an overview on which and how many information is shared with whom. Notably, this creates an atmosphere of transparency, which in turn may lead to the fact that users view a certain online environment as a safe environment for information disclosure (Krasnova et al., 2009). As we expect the DIMS to offer more control mechanisms than the SSO-scheme, we hypothesize:

H7. *For users of DIMS, perceived transparency of self-disclosed data online is a stronger predictor of willingness to self-disclose data than for users of CIMS.*

Studies have shown the positive effects of users' perceived transparency on trust in different settings (e.g., e-commerce) that leads to a positive attitude towards an online service (Dwyer, Hiltz and Passerini, 2007; Ionescu, 2016). As already mentioned, we expect transparency to be higher in the DIMS. However, we hypothesize a direct effect of perceived transparency on attitude towards the DIMS, because no central, trusted party exists in the DIMS. Thus, we conclude:

H8. *For users of DIMS, perceived transparency of self-disclosed data online is a stronger predictor of attitude towards the IMS than for users of CIMS.*

Various studies showed that personal information used as means of authentication by an SSO scheme provider are prone to attacks and exhibits several vulnerabilities (Sun and Beznosov, 2012; Wang et al., 2012). Whereas there is no study on the security of data that are transferred via a DIMS, the decentralization of personal information may reduce the incentive of attackers to seize information of one person compared to the possibilities that open up for attackers, when information of thousands of users is comprised in a central database. We conclude that the willingness to disclose information is greater using the DIMS, whereas self-disclosure is a distinct but strong predictor of a positive attitude towards the DIMS and, thus, a strong predictor towards the intention to use DIMS compared to the CIMS (Ledbetter et al., 2011). Thus, we conclude:

H9. *For users of DIMS, willingness to self-disclose data online is a stronger predictor of attitude towards the IMS than for users of CIMS.*

We want to emphasize that we are aware of the fact that the construct of perceived privacy risks is often included in research models trying to capture the factors influencing self-disclosure in online environments. We intentionally excluded perceived privacy concerns from our analysis, as several studies

showed that there is no direct influence of perceived privacy risks on self-disclosure behavior (Taddicken 2014). In particular, Taddicken (2014) shows that privacy concerns hardly affect self-disclosure behavior, i.e., concerns for the security of one's private information is not necessarily accompanied by a corresponding behavior.

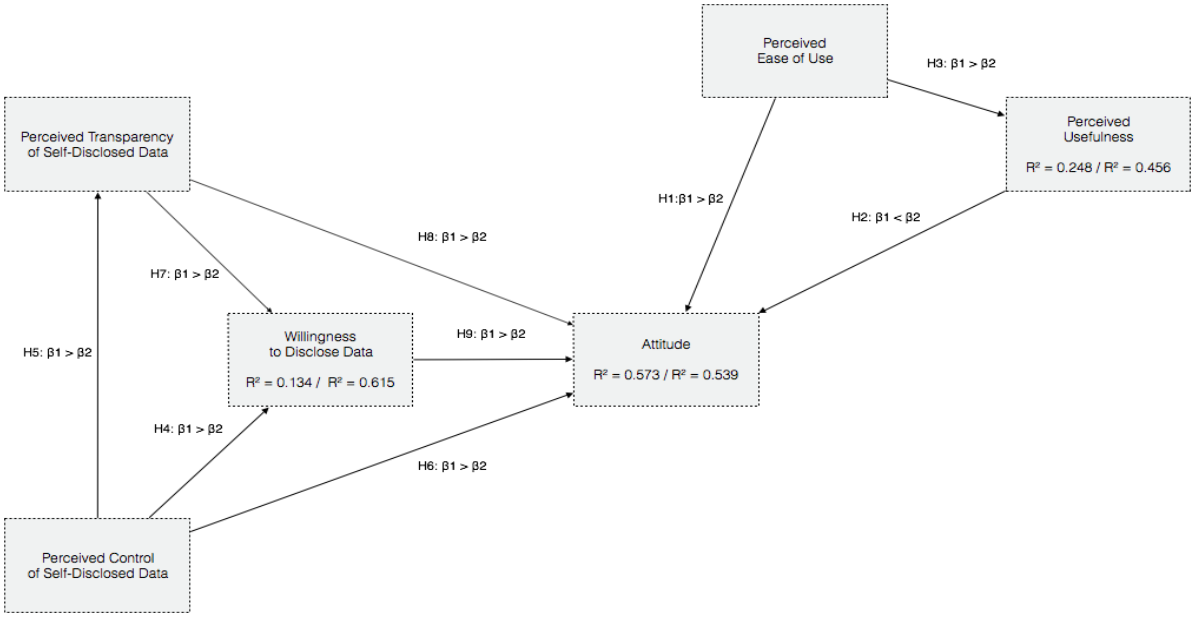


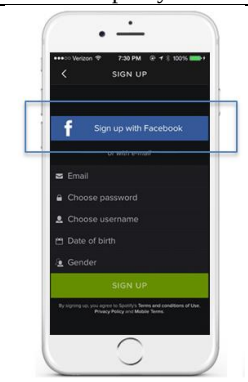
Figure 1. Research Model (1 = DIMS; 2= CIMS)

3 Methodology and Results

3.1 Measures and Data Collection

To test the hypotheses a standardized questionnaire was designed, which shows mock-ups of the CIMS and the DIMS. The mock-ups were designed to put our participants in the situation to use either a CIMS *or* a DIMS in a mobile environment (please note that, generally, CIMS and DIMS can be applied at any devices with Internet connectivity. Thus, the use of the IMSs on the cell phone is only one possibility, chosen to simulate the use of the systems). Participants got to see only one version of the mock ups. In particular, we divided our participants in two groups: Group 1 received a questionnaire with descriptions on the use of a CIMS, using the example of an SSO-scheme. Group 2 received a questionnaire explaining and visualizing the use of a DIMS. To visualise the functionality of the two IMSs, we decided to use the sign-in scenario of the popular music, podcast, and video streaming service Spotify as a research set up. Figure 2 contains the descriptions as well as the mock-ups itself, used to make participants familiar with the respective interfaces.

One step, which is part of the authentication process as shown in Figure 2, is that participants must allow Spotify to access some personal data, which is defined as a prerequisite to use Spotify's service. SSO's require that users' data provided through the SSO must also flow to the identity provider. Thus, the identity provider can easily gather user information by linking various websites that the user visits, track users' activities such as his or her buying habits and transaction history without permission from the user (Khattak et al. 2011). While using a DIMS does probably not prevent Spotify or other parties from gathering additional user information, at least, it provides more transparency over data that is collected. Eventually, refusing to disclose certain information would restrict users' access to services like those offered by Spotify. The functionalities of the CIMS and DIMS were described in a detailed way. While providing detail descriptions bears the risks of influencing the answers of the participants, this was necessary given the novelty of the tested IMSs, especially about the DIMS. A lack of information on how the IMSs work, in turn, would bear the risks that participants answer the questionnaire without sufficient knowledge to assess the respective mock-up, leading to biased results.

<table>
<tr><th></th><th>Group 1: CIMS Functionality Description</th><th>Group 2: DIMS Functionality Description</th></tr>
<tr><td>Set up</td><td colspan="2">You want to register at Spotify for the first time, which is a music, podcast, and video streaming service provider. For the registration, Spotify needs personal information such as your name, your address, your email. Maybe Spotify is also interested in additional information such as your music preferences or your general interests.</td></tr>
<tr><td>Functionality description</td><td>Nowadays, there exist various opportunities to register at Spotify. For example, you can register manually, by typing in all relevant information and setting a new password (traditional log in). Another option that is regularly offered is a so-called single-sign on (SSO) schemes, meaning that you register yourself at Spotify by using your Facebook (FB) profile. SSO schemes are possible since your FB profile already contains various relevant information that is needed for your registration at Spotify. This speeds up the registration process, but you need to trust FB as the third party when information is disclosed. The only information you receive is that Facebook grants Spotify access to your profile and that Spotify is not allowing to post on your wall. In practice, an SSO scheme on Spotify looks like in the following:</td><td>Nowadays, there exist various opportunities to register at Spotify. For example, you can use a decentralized identity management system (DIMS), which can but does not have to be based on a blockchain. Using a DIMS for registration means that you do not need to trust FB as a third party when signing in at Spotify, because you are the owner of your data in such systems. Since you are the owner, you can restrict or grant access to your data to Spotify or another service provider purposefully. Moreover, you get to know in which data Spotify and other service provider are interested in and you can choose whether you are willing to accept the collection of particular data or not. In practice, an App for a DIMS could look like this:</td></tr>
<tr><td>Mock ups</td><td> 

Step 1: The App informs you that Spotify offers you the opportunity to sign in with your Facebook profile.
Step 2: You need to confirm that Facebook grants Spotify access to your profile information, but is not allowed to post content on your wall.
Step 3: You click on the accept button and you are immediately registered at Spotify.</td><td> 

Step 1: You need to confirm that Facebook grants Spotify access to your profile information, but is not allowed to post content on your wall.
Step 2: You click on the accept button and you are immediately registered at Spotify.
Step 3: You decide, who has access to which of your data and to what level of detailedness (e.g., you can verify your identity without revealing details behind that identity).</td></tr>
</table>

Figure 2. Visualisation of the centralised and decentralised identity management system

The first section of the questionnaire contained construct questions measuring *Perceived Ease of Use*, *Perceived Usefulness* and *Attitude* towards using the IMS. The constructs used to test the proposed research model are based on existing literature and are available in the appendix, along with the list of items. In the second part, IMS related questions to measure users' *Perceive Transparency* and *Perceived Control of Self-Disclosed Data* as well as users' *Willingness to Disclose Data* were asked. The third section consisted of questions related to demographics, namely to age, gender, highest education achieved and working status. The paper form questionnaire was answered by students participating in three bachelor courses with information system related content of a German university in the mid of the 2017/2018 winter term. The approximate time needed to answer the questionnaire amounted to 17 minutes. Data collection took place between October and November 2017. In total, 131 completed surveys were received: 60 participants answered questions related to the use of CIMs, whereas 71 evaluate DIMs usage. 53,4% of the participants were female. Most of the participants were younger than 25 (68,7%) or between the age of 26 and 35 (29%). For 60 % of all particpants, the highest educational status achieved was matura, 29,8 % already had a bachelor degree.

3.2 Measurement Model

For the assessment and evaluation of the reflective measurement model, several criteria need to be tested (see Henseler et al. 2009). Construct reliability was assessed by applying the test for composite reliability (CR), which is an indicator of internal consistency between measurements of a latent variable. Values higher than 0.7 indicate that all items in each latent variable form a single latent construct (see Hair et al. 2006). This test can be seen as more precise than the traditional criterion for internal consistency (i.e., Cronbach's Alpha), as the latter assumes that all indicators are equally weighted, which underestimates the internal consistency reliability of latent variables (Chin 1998).

	CIMS/DIMS							
	Loadings	**CR**	**AVE**	**Latent Variable Correlations**				
				ATT	**PEOU**	**PCDD**	**PTDD**	**PU**	**WDD**
ATT1	0.955/ 0.961	0.959/ 0.962	0.922/ 0.927	**0.960/ 0.963**					
ATT2	0.965/ 0.964								
PEOU1	0.870/ 0.908	0.868/ 0.929	0.768/ 0.867	0.200/ 0.662	**0.877/ 0.931**				
PEOU2	0.876/ 0.926								
PEOU3	0.873/ 0.926								
PCDD1	0.938/ 0.934	0.906/ 0.943	0.762/ 0.847	0.197/ 0.314	0.049/ 0.095	**0.873/ 0.920**			
PCDD2	0.810/ 0.929								
PTDD1	0.837/ 0.875	0.894/ 0.888	0.738/ 0.727	0.239/ 0.532	0.284/ 0.579	0.092/ 0.185	**0.859/ 0.852**		
PTDD2	0.919/ 0.872								
PTDD3	0.818/ 0.809								
PU1	0.756/ 0.884	0.861/ 0.885	0.676/ 0.720	0.683/ 0.289	0.082/ 0.216	0.498/ 0.675	0.126/ 0.194	**0.822/ 0.848**	
PU2	0.800/ 0.865								
PU3	0.903/ 0.794								
WDD1	0.911/ 0.957	0.915/ 0.972	0.781/ 0.920	0.436/ 0.629	0.337/ 0.755	0.072/ 0.180	0.233/ 0.610	0.259/ 0.291	**0.884/ 0.959**
WDD2	0.888/ 0.964								
WDD3	0.852/ 0.955								

Table 2. Results of the measurement model analysis

As shown in Table 2, the CR-values range from 0.852 to 0.9632, which exceeds the recommended threshold 0.7 (Hair et al. 2006). We assessed indicator reliability by checking factor loadings (Johnson et al. 2006). As shown in Table 2, all items have loadings above 0.7, which indicates that the indicators are reliable. Construct validity, which measures whether the indicators explain their respective latent variables, can be assessed through convergent validity and discriminant validity (Henseler et al. 2009). For the assessment of convergent validity, we used the average variance extracted (AVE) (Fornell and Larcker, 1981). As shown in Table 2, the AVE of each latent variable ranges from 0.676 to 0.927, which is above the recommended threshold of 0.5 (Fornell and Larcker, 1981). For the assessment of discriminant validity, we referred to the Fornell-Larcker criterion (Fornell and Larcker 1981; Hair et al. 2006). This criterion is evaluated using a comparison of the square root of the AVE of every latent variable with the correlation coefficients among the latent variables, where the former should be higher than the latter (Fornell and Larcker, 1981; Hulland, 1999). As shown in Table 2, this is the case for all the variables. Furthermore, the bootstrapping procedure for assessing measurement invariance across the group-specific PLS path models was used (Rigdon et al. 2010). As shown in Table 3, the results of the composite reliabilities and AVEs do not differ significantly between the DIMS and the CIMS. Thereby, the measurement model invariance is established (Sarstedt et al., 2011).

Latent Variable	Quality Criterion	CIMS/DIMS				
		Original Sample	Standard Error	|Diff|	t-value	p-value
Attitude	CR	0,959/ 0,962	0,014/ 0,012	0,003	0,1640	0,8701
	AVE	0,922/ 0,927	0,025/ 0,023	0,005	0,1483	0,8824
Perceived Ease of Use	CR	0,868/ 0,929	0,125/ 0,024	0,061	0,4833	0,6299
	AVE	0,768/ 0,867	0,100/ 0,042	0,099	0,9203	0,3596
Perceived Control	CR	0,906/ 0,943	0,037/ 0,016	0,037	0,9254	0,3570
	AVE	0,762/ 0,847	0,070/ 0,037	0,085	1,0823	0,2817
Perceived Transparency	CR	0,894/ 0,888	0,058/ 0,034	0,006	0,0900	0,9285
	AVE	0,738/ 0,727	0,072/ 0,065	0,011	0,1143	0,9092
Perceived Usefulness	CR	0,861/ 0,885	0,033/ 0,024	0,024	0,5929	0,5546
	AVE	0,676/ 0,720	0,056/ 0,045	0,044	0,6173	0,5384
Willingness to Disclose	CR	0,915/ 0,972	0,077/ 0,007	0,057	0,7434	0,4590
	AVE	0,781/ 0,920	0,093/ 0,018	0,139	1,4797	0,1421

Table 3. Test for measurement invariance

3.3 Structural model

Several criteria need to be tested for an assessment of the structural model. These included coefficient of determination (R2), estimates for path coefficients and effect sizes (f2) (see Chin 1998; Henseler et al. 2009). The first necessary criterion to evaluate is the coefficient of determination (R2 value), which represents the variance of the latent endogenous variable explained by the antecedent exogenous variables (Chin 1998; Hulland 1999). R2 values of 0.67 for endogenous latent variables can be described as "substantial," whereas values of 0.33 and 0.19 are rated as "moderate" and "weak," respectively (Chin 1998). The R2 value of the endogenous variable Willingness to Disclose Data amounts to 13.4% for CIMS (61.5% for DIMS), and indicates a weak (substantial) explanatory power of the exogenous variables. The R2 value of the endogenous variable Attitude amounts to 57,3% for CIMS (53,9% for DIMS) and indicates a substantial explanatory power (both) of the exogenous variables (Chin 1998).

To test the hypotheses, we adopted a non-parametric procedure, named PLS-MGA (multi- group analysis) (Henseler 2012). First, the PLS structural model for each subsample was estimated. The second and third columns of Table 4 show the path coefficients and their significant levels for both groups. Second, each path coefficient estimate of the group DIMS users (ß1) was compared with the corresponding estimate of the group of CIMS users (ß2). The results indicate that all hypotheses related to the variable perceived control of self-disclosed data (H4 to H6) are supported. As shown in the second column of Table 4, the influence of perceived control of self-disclosed data on attitude is stronger for DIMS users (ß1=0,425, p<0.01) than for CIMS users (ß2=0,046, n.s.). And as shown in the sixth column of Table 4, the path coefficients do differ significantly between the two models (p=0,983). Thus, H6 is supported. The influence of perceived control of self-disclosed data on perceived transparency of self-disclosed data is also as hypothesized stronger for DIMS users (ß1=0,579, p<0,01) than for CIMS users (ß2=0,284, p<0,05). Again, the path coefficients differ significantly be- tween the two models (p=0,984). Furthermore, the influence of perceived control of self-disclosed data on users' willingness to disclose data (H4) is stronger for DIMS users (ß1= 0,604, p<0,01) than for CIMS users (ß2=0,294, p<0,1) and the difference between the path coefficients between the two models is also statistically significant (p=0,967). The influence of perceived ease of use on attitude is stronger for DIMS users (ß1=0,254, p<0,01) than for CIMS users (ß2=-0,177, n.s.). In the case of CIMS users, this influence is surprisingly negative meaning, that the easier the system is perceived to be used the less the impact on attitude towards the CIMS. Hence, the sixth column of Table 4 indicates that the path coefficients do differ significantly between the two models (p=0,984). However, even though the influence of perceived ease of use on perceived usefulness is again stronger for DIMS users (ß1=0,675, p<0,01) than for CIMS users (ß2=0,498, p<0,01), the hypothesis H3 is not supported as the difference of path coefficients between the two models is not statistically significant (p=0,916). Surprisingly, the influence of perceived usefulness on attitude is negative and hence much weaker for DIMS users (ß1=-0,058 n.s.) than for CIMS users (ß2=0,695, p<0,01). In H2 we hypothesized, that this influence is stronger for DIMS users. Hence, even though the difference is statistically significant (p=0,000), our hypothesis is not supported.

Path	Coefficients		Hypotheses	| CIMS - DIMS |	p-Value (CIMS vs. DIMS)	Hypothesis Support
	CIMS	DIMS				
PEOU → ATT	-0,177 n.s.	0,254 **	**H1**: β1 > β2	0,431	**0,984**	Supported
PU →ATT	0,695 ***	-0,058 n.s.	**H2**: β1 < β2	0,753	**0,000**	Not Supported
PEOU →PU	0,498 ***	0,675 ***	**H3**: β1 > β2	0,177	0,916	Not Supported
PCDD → WDD	0,294 *	0,604 ***	**H4**: β1 > β2	0,310	**0,967**	Supported
PCDD → PTDD	0,284 **	0,579 ***	**H5**: β1 > β2	0,295	**0,984**	Supported
PCDD → ATT	0,046 n.s.	0,425 ***	**H6**: β1 > β2	0,379	**0,983**	Supported
PTDD → WDD	0,149 n.s.	0,260 ***	**H7**: β1 > β2	0,111	0,730	Not Supported
PTDD → ATT	0,101 n.s.	0,127 n.s.	**H8**: β1 > β2	0,025	0,541	Not Supported
WDD → ATT	0,230 **	0,202 n.s.	**H9**: β1 > β2	0,028	0,434	Not Supported
Note: *** p < 0,01, ** < 0,05, * p <0,1 n.s. = not significant						

Table 4. Multi-group comparison test results

Perceived transparency of self-disclosed data has only a small influence on attitude, and this impact is for both models not statistically significant. Although as hypothesized, the influence is (slightly) stronger for DIMS users (ß1=0,127, n.s.; ß2=0,101 n.s.) also the difference between the path coefficients is similarly not statistically significant (p=0,541). The influence of perceived transparency of self-disclosed data on the willingness to disclose data is considerably stronger for DIMS users (ß1=0,260, p<0,01) than for CIMS users (ß2=0,149, n.s.). However, the path coefficients PTDD →WDD do not differ significantly (p=0,730).

Lastly, the influence of willingness to disclose data on attitude is others than hypothesized weaker for DIMS users (ß1=0,202, n.s.) than for CIMS users (ß2=0,230, p<0,05). The path coefficients again do not differ significantly (p=0,434). Hence the hypothesis H9 is not supported.

Mediation Paths	PTDD --> WDD --> ATT (IV = PTDD / M = WDD / DV = ATT)		PEOU --> PU --> ATT (IV = PEOU / M = PU / DV = A TT)		PCDD --> WDD --> ATT (IV = PCDD / M = WDD / DV = ATT)	
	CIMS	DIMS	CIMS	DIMS	CIMS	DIMS
IV--> DP	β= 0,273 p<0.1	β= 0,532 p<0.01	β= 0,243 n.s	β= 0,319 p< 0,01	β= 0,262 n.s.	β= 0,662 p< 0,01
IV --> MED	β= 0,300 n.s.	β= 0,616 p<0.01	β= 0,547 p< 0,01	β= 0,675 p< 0,01	β= 0,351 p< 0,1	β= 0,755 p< 0,01
IV --> DP	β= 0,153 n.s.	β= 0,233 n.s.	β= -0,190 n.s	β= 0,219 n.s.	β= 0,087 n.s.	β= 0,435 p< 0,01
IV --> MED	β= 0,240 p<0.01	β= 0,611 p<0.01	β= 0,498 p< 0,01	β= 0,675 p< 0,01	β= 0,353 p< 0,1	β= 0,755 p< 0,01
MED --> DP	β= 0,409 p<0.01	β= 0,486 p<0.01	β= 0,777 p< 0,01	β= 0,143 n.s.	β= 0,399 p< 0,01	β= 0,301 p< 0,1
Sobel test	Z = 1,886 (n.s.)	**Z = 2,006 (p<0.05)**	**Z = 3,687 (p<0.01)**	Z = 0,930 (n.s.)	Z = 1,467 (n.s.)	**Z = 3,178 (p<0.01)**
Mediation Type	No Mediation	Full	Full	No Mediation	No Mediation	Partial

Table 5. Mediation Effects

Construct	**f2 - Effect Size**		**Effect**	
	CIMS	**DIMS**	**CIMS**	**DIMS**
PCDD --> ATT	0,0040	0,1580	none	moderate
PCDD --> PTSD	0,0880	0,5050	weak	large
PCDD --> WDSN	0,0920	0,6300	weak	large
PEOU --> ATT	0,0550	0,0740	weak	weak
PEOU -->PU	0,3300	0,8390	weak	large
PTSD --> ATT	0,0210	0,0200	none	none
PTSD --> WDSN	0,0240	0,1170	none	weak
PU --> ATT	0,7920	0,0040	large	none
WDSN --> ATT	0,1000	0,0330	weak	weak

Table 6. Effect sizes

Based on the results of the t-statistics, which highlighted that perceived control of self-disclosed data failed to predict attitude for CIMS users in the presence of willingness to disclose data, an analysis into a potential mediation effect through the willingness to disclose data was conducted (Baron and Kenny 1986). Additionally, a Sobel test to assess the significance of the mediation effect (i.e., whether the indirect effect of the exogenous variable through the mediator variable is significant) was conducted (Sobel 1982). As shown in Table 5, the results demonstrate that for DIMS users, willingness to disclose data fully mediates the relationship between perceived transparency of disclosed data and attitude and partially between perceived data control and attitude. For CIMS users, perceived usefulness fully mediates perceived ease of use and attitude, whereas no such effect can be observed for DIMS users. Lastly, for assessing the structural model, the effect size is captured, which measures the effect of an exogenous latent variable on an endogenous latent variable and can be obtained by Choens's f2 (Chin 1998, Cohen 1988). The change in the R2 of the endogenous latent variable is calculated by estimating the structural model twice, for when an exogenous variable is used and when it is not used. Values of 0,02 indicate that the predictor variable has a "weak" effect size on the endogenous variable, whereas the values of 0,15 and 0,35 indicate a "moderate" effect size, respectively (Chin, 1998; Cohen 1988). As shown in Table 6 the effect sizes of perceived control of self-disclosed data on the endogenous variable attitude are moderate for DIMS users, whereas there is no

effect for CIMS users. Considering the effects of perceived control of self-disclosed data on perceived transparency and willingness to disclose data, large effects can be observed for DIMS users and weak effects for CIMS users. In the case of perceived ease of use, the effect on attitude is for both groups weak. The effect sizes of perceived ease of use on perceived usefulness vary between groups, as there is a weak effect for CIMS users and large effect for DIMS users. Perceived transparency of self-disclosed data has no effects on attitude for both groups. However, a weak effect can be observed for perceived transparency of self-disclosed data on willingness to disclose for DIMS users. The effect sizes of perceived usefulness on the endogenous variable attitude are large for CIMS users, whereas for DIMS users no effect can be observed. Finally, the weak effects of willingness to disclose data on attitude can be observed across both groups.

4 Discussion - The Paradox of Control

We investigated the effect of CIMSs and DIMSs on users' self- presentation behavior by proposing a research model that combines factors that influence user willingness on disclosure behavior, as well as their attitude towards the respective IMS. Hypotheses H1 to H3 examine the relationship between the design specific variables perceived ease of use, perceived usefulness and attitude, whereby the data supported H1. This reveals that for DIMS the *ease of use* is a stronger predictor of attitude towards an IMS than for CIMS, whereas for CIMS this relationship was negative. This effect is of great practical importance, indicating that an interface design reduced to elementary characteristics may negatively affects users' feeling towards using an IMS. For users of the CIMS, the data revealed that *perceived usefulness* outweighs the negative effect of *perceived ease of use* leading to an overall strong positive effect on attitude. Contrarily, users of the DIMS exhibit a reverse behavior: the positive effect of *perceived ease of use* outweighs the negative, but almost zero effect of *perceived usefulness* on attitude.

The data also reveal that all control related hypotheses are supported. While perceived control of self-disclosed data has a positive effect on attitude towards the IMS on both groups, the effect for the CIMS users is almost zero and not significant. This result is in line with the design features of the respective IMS, as users of CIMSs are not provided with information about the data revealed, which implies that they have no opportunity to control either self-disclosed data or data collected and shared by the SSO scheme provider. Moreover, H5 is supported as the perceived control of data is provided in the case of DIMS users and, thus, is a stronger predictor for its influence on perceived transparency on self-disclosed data. Most importantly, H4 is supported by the data, which means that perceived control of self-disclosed data has a positive effect on self-disclosing behavior that is stronger for users of the DIMS than for users of CIMS. This is in line with existing literature, stating that users that have perceived control may be less worried about disclosure than users without the feeling of control (Malhotra et al., 2004; Brandimarte et al., 2012). Consequently, perceived control over self-disclosed information seems to affect users' disclosure behavior more than the actual design features (perceived ease of use, perceived usefulness) of the DIMS. These results are expected to hold in other contexts, i.e. when a user applies a CIMS or DIMS in other than the proposed mobile environment. These theoretical results also have practical implications. The negative effect of ease of use in the case of CIMS indicates that IMS user interfaces must reflect the users' requirements regarding control and privacy protection. SSO schemes that are designed to increase user application through a simplified user interface, however, do not consider the fact that a system that is perceived as extremely easy to use might have a negative effect on users' feelings towards the IMS. Moreover, the study leads to recommendations towards possible use cases of DIMS within service that require a high level of information disclosure as well as a high degree of users' perceived control. For instance, DIMS could open up new opportunities for e-government applications that require the disclosure of accurate and identifiable user information.

5 Conclusion and Outlook

The first conclusion of this paper is that the design of the IMS whether centralized or decentralized has a significantly different effect on user disclosing behavior. User interfaces of IMSs need to take ac-

count of user requirements that possibly negatively influence their feelings towards an IMS. When considering the unacceptably high failure rate for newly developed information systems (Davis and Venkatesh, 2004) our study shows that it is highly beneficial to verify and test requirements by using pre-prototypes of IMSs based on users' evaluations of its specifications. The second conclusion is that perceived control of self-disclosed data is a strong predictor of perceived transparency as well as user willingness to disclose data and in the case of DIMS, also on users' attitude. This is not surprising as the CIMS with its structure and interface does not provide a control mechanism to users. Hence, this effect on attitude cannot be observed in the case of CIMS.

The paper also exhibits limitations that refer to the provided mock-ups, which are an *existing* (SSO-scheme) and a *fictional* (DIMS) application. Features of the fictional DIMS were combined by screening whitepapers to receive a mock up that, on average, captures proposed features of DIMSs. The mock-ups were described in a detailed fashion, which we supposed s necessary given the novelty of the DIMS. These detailed descriptions may have influenced the results of this study. However, one indicator that this is not the case are the results concerned with perceived transparency over self-disclosed data. Despite we purposefully stated in the mock ups descriptions that DIMS are expected to provide greater transparency over data, no significant difference between the two groups emerged. A further limitation of our analysis is the focus on young adults of an average age of younger than 35. This might have affected the results although we cannot find evidence for that in our dataset. We purposefully omit privacy concerns from our analysis as several researchers showed that privacy concerns only have minor effects on users' overall self-disclosure behavior (e.g., Taddicken 2014). Nevertheless, we are aware of the fact that other variables (e.g., perceived social relevance, the number of online services used) may moderate this relation. Consequently, a replication of this study needs to be done, taking into account the effects of privacy concerns and moderators on self-disclosure behavior. Despite these limitations, our study reveals interesting results that can guide future research into DIMS and the disclosure behavior in general.

Consequently, future research needs to take up these limitations by extending the sample towards an increasingly heterogeneous group of participants and by tracking the developments in the field of DIMS interface design.

6 Appendix

Construct	Items	Source & Scale
Attitude [ATT]	ATT 1: Using the SSO-scheme/DIMS is a ... Scale: [Bad idea – Good Idea] ATT 2: I ... the idea of using the SSO-scheme/DIMS. Scale: [Dislike - Like]	Davis et al. 1989 / Fishbein and Ajzen 1975
Perceived ease of use [PEU]	PEU1: Learning to operate the SSO-scheme/DIMS would be easy for me. PEU2: My interaction with the SSO-scheme/DIMS would be clear and understandable. PEU3: I would find the SSO-scheme/DIMS easy to use.	*Scale: [Totally Disagree – Agree]* Davis 1989 / Davis et al. 1989
Perceived usefulness [PU]	PU1: Using the SSO-scheme/DIMS would enable me to accomplish tasks more quickly. PU2: Using the SSO-scheme/DIMS would enhance my effectiveness. PU3: I would find the SSO-scheme/DIMS useful.	
Perceived control of self-disclosed data [PCDD]	PCDD1: I have control and autonomy over decisions about what information I disclose. PCDD2: I have control and autonomy over decisions which self-disclosed information third parties receive.	Taylor and Todd (1995)
Perceived transparency of self-disclosed data [PTDD]	PTDD1: The SSO-scheme/DIMS allows me to keep an overview of the data that I reveal. PTDD2: The SSO-scheme/DIMS allows me to change information about myself. PTDD3: The SSO-scheme/DIMS allows me to delete information about myself.	Rawlins (2008)
Willingness to self-disclose data [WDD]	To what extent are you willing to provide relevant data in these cases? WDD1: Use free social networks such as Facebook that require me to submit accurate and identifiable information. WDD2: Use free chat services such as WhatsApp by means of which I interchange accurate and identifiable information about me. WDD3: Use free social networks such as Xing or LinkedIn that require me to disclose predominantly job related information.	*Scale: [Not at all – Very much]* Dinev and Hart (2006)

References

Acquisti, A. and Gross, R. (2006). *"Imagined communities: Awareness, information sharing, and privacy on the facebook."* In: Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), pp. 36–58.

Attrill, A. and Jalil, R. (2011). *"Revealing only the superficial me: Exploring categorical self-disclosure online."* In: Computers in Human Behavior, pp. 1634–1642.

AuthenticID Whitepaper (2017). URL: https://icosbull.com/whitepapers/1354/AuthenticID_whitepaper.pdf

Baars, D. (2016). "*Towards Self-Sovereign Identity using Blockchain Technology.*" Master Thesis. University of Twente.

Baron, R. M. and Kenny, D. a (1986). *"The moderator-mediator variable distinction in social psychological research: conceptual, strategic, and statistical considerations."* In: Journal of personality and social psychology, 51(6), pp. 1173–1182.

Benford, S. et al. (2006). *"Can you see me now?"* In: ACM Transactions on Computer-Human Interaction, 13(1), pp. 100–133.

Bertino, E., Paci, F., Ferrini, R., & Shang, N. (2009). *"Privacy-preserving digital identity management for cloud computing.*" In: IEEE Data Eng. Bull., 32(1), 21-27.

BotChain Whitepaper (2017). URL: https://botchain.talla.com/whitepaper.pdf (visited on 09/10/2018)

Boyd, D. M. and Ellison, N. B. (2007). *"Social network sites: Definition, history, and scholarship."* In: Journal of Computer-Mediated Communication, 13(1), pp. 210–230.

Brandimarte, L., Acquisti, A. and Loewenstein, G. (2012). *"Misplaced Confidences: Privacy and the Control Paradox."* In: Social Psychological and Personality Science, 4(3), pp. 340–347.

Chin, W. W. (1998). *"The Partial Least Square Approach to Structural Equation Modeling."* In: Modern Methods for Business Research, pp. 295–336.

Civic Whitepaper (2018). https://www.civic.com/wp-content/uploads/2018/05/Token-Behavior-Model-May-16-2018.pdf (visited on 09/10/2018)

Clauß, S., Kesdogan, D. and Kolsch, T. (2005). *"Privacy Enhancing Identity Management : Protection Against Re-identification and Profiling."* In: Proceeding: DIM '05 Proceedings of the 2005 workshop on Digital identiry management, (November), pp. 84–93.

Clercq, J. De (2002). *"Single Sign-On Architectures."* In: Infrastructure Security - International Conference, InfraSec 2002 Bristol, UK, October 1–3, 2002 Proceedings, pp. 40–58.

Dashlane 2015. *Online overload – Worse Than You Thought. When it comes to dealing with our online presence the struggle is real. URL: https://blog.dashlane.com/wp-content/uploads/2015/07/MailboxSecurity_infographic_EN_final1.jpg (visited on 11/01/2018)*

Davis, F. D., & Venkatesh, V. (2004). *"Toward preprototype user acceptance testing of new information systems: implications for software project management."* In: IEEE Transactions on Engineering management, 51(1), 31-46.

Davis, F. D., Bagozzi, R. P., & Warshaw, P. R. (1989). *"User acceptance of computer technology: a comparison of two theoretical models."* In: Management science, 35(8), 982-1003.

Derlega, V. J. and Grzelak, J. (1979). Appropriateness of self-disclosure, Self-disclosure: Origins, patterns, and implications of openness in interpersonal relationships. URL: http://www.tandfonline.com/doi/abs/10.1080/07362999408809355. (visited on 15/10/2018)

Dinev, T. and Hart, P. (2006). *"An extended privacy calculus model for e-commerce transactions."* In: Information Systems Research, 17(1), pp. 61–80.

Dinev, T., & Hart, P. (2006). *"An extended privacy calculus model for e-commerce transactions."* In: Information systems research, 17(1), 61-80.

Diro Whitepaper (2018). https://docs.wixstatic.com/ugd/fae167_a8d731c7a2484c33847e588a0dd60f04.pdf (visited on 09/10/2018)

Dwyer, C., Hiltz, S. R. and Passerini, K. (2007). *"Trust and privacy concern within social networking sites: A comparison of Facebook and MySpace."* In: Americas Conference on Information Systems (AMCIS), pp. 339–350.

Fishbein, M., & Ajzen, I. (1975). *"Belief, attitude, intention and behavior: An introduction to theory and research."*

Fornell, C. and Larcker, D. F. (1981). *"Structural Equation Models with Unobservable Variables and Measurement Error: Algebra and Statistics."* In: Journal of Marketing Research, 18(3), p. 382.

Fromknecht, C. and Velicanu, D. (2014). *"A Decentralized Public Key Infrastructure with Identity Retention."* In: Cryptology ePrint Archive, pp. 1–16.

Goffman, E. (1959). *"The Presentation of Self in Everyday Life."* In: Teacher, 21(5), p. 259.

Greene, K., Derlega, V. J. and Alicia, M. (2006). Self-disclosure in personal relationships. The Cambridge handbook of personal relationships, pp. 409–427.

Hair, J. F. et al. (2010). Multivariate Data Analysis. Vectors, p. 816.

Hansen, M., Berlich, P., Camenisch, J., Clauß, S., Pfitzmann, A., & Waidner, M. (2004). *"Privacy-enhancing identity management*." In: Information security technical report, 9(1), 35-44.

He, W. (2000). *"Single Sign On."* In: Networks, 33, pp. 51–58.

Henseler, J. (2012). *"Why generalized structured component analysis is not universally preferable to structural equation modelling."* In: Journal of the Academy of Marketing Science, 40(3), pp. 402–413.

Henseler, J., Ringle, C. M. and Sinkovics, R. R. (2009). *"The use of Partial Least Squares Path Modeling in International Marketing."* In: Advances in International Marketing, 20(2009), pp. 277–319.

Honestis Whitepaper (2017). URL: https://icosbull.com/whitepapers/1583/Honestis_Network_whitepaper.pdf

Hulland, J. (1999). *"Use of partial least squares (PLS) in strategic management research: a review of four recent studies."* In: Strategic Management Journal, 20(2), pp. 195–204.

IBM (2017). Trust me: Digital identity on blockchain. URL: https://public.dhe.ibm.com/common/ssi/ecm/gb/en/gbe03823usen/GBE03823USEN.PDF (visited on 20/09/2018)

Ionescu, L. (2016). *"E-Government and Social Media as Effective Tools in Controlling Corruption in Public Administration."* In: Economics, Management & Financial Markets, 11(1), pp. 66–72.

Jacobs, R. S., Hyman, M. R. and McQuitty, S. (2001). *"Exchange-specific self-disclosure, social self-disclosure, and personal selling."* In: Journal of Marketing Theory and Practice, 9(1), pp. 48–62.

Joinson, A. N. (2001). *"Self-disclosure in computer-mediated communication: The role of self-awareness and visual anonymity."* In: European Journal of Social Psychology, 31(2), pp. 177–192.

Joinson, A. N. et al. (2010). *"Privacy, trust, and self-disclosure online."* In: Human-Computer Interaction, 25(1), pp. 1–24.

Joinson, A. N. et al. (2012). Oxford Handbook of Internet Psychology. Oxford Handbook of Internet Psychology.

Jones, K. S. (2003). *"Privacy: what's different now?"* In: Interdisciplinary Science Reviews, pp. 287–292.

Jøsang, A. and Pope, S. (2005). *"User centric identity management."* In: AusCERT Asia Pacific Information Technology Security Conference, pp. 1–13.

Kaplan, A. M. and Haenlein, M. (2010). *"Users of the world, unite! The challenges and opportunities of Social Media."* In: Business Horizons, 53(1), pp. 59–68.

Khattak, Z. B., Ab Manan, J. L. and Sulaiman, S. (2011): "Analysis of Open Environment Sign-In Schemes- Privacy Enhanced & Trustworthy Approach." Journal of Advances in Information Technolgoy 2(2), pp. 109-121.

Kokolakis, S. (2017). *"Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon."* In: Computers and Security, pp. 122–134.

Krasnova, H. et al. (2009). *"Privacy concerns and identity in online social networks."* In: Identity in the Information Society, 2(1), pp. 39–63.

Krasnova, H. et al. (2010). *"Online social networks: Why we disclose?"* In: Journal of Information Technology, 25(2), pp. 109–125.

Krasnova, H. et al. (2013). *"Envy on Facebook: A Hidden Threat to Users' Life Satisfaction?"* In: 11th International Conference on Wirtschaftsinformatik, (March), pp. 1–16.

Ledbetter, A. M. et al. (2011). *"Attitudes Toward Online Social Connection and Self-Disclosure as Predictors of Facebook Communication and Relational Closeness."* In: Communication Research, 38(1), pp. 27–53.

Malhotra, N. K., Kim, S. S. and Agarwal, J. (2004). *"Internet users' information privacy concerns (IUIPC): The construct, the scale, and a causal model."* In: Information Systems Research, pp. 336– 355.

Meng, M. and Agarwal, R. (2007). *"Through a glass darkly: Information technology design, identity verification, and knowledge contribution in online communities."* In: Information Systems Research, 18(1), pp. 42–67.

Moore, G. C. and Benbasat, I. (1991). *"Development of an instrument to measure the perceptions of adopting an information technology innovation."* In: Information Systems Research, 2(3), pp. 192–222.

Nakamoto, S. (2008). *"Bitcoin: A Peer-to-Peer Electronic Cash System." In:* Www.Bitcoin.Org, p. 9.

Narayanan, A. et al. (2016). Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction. Princeton: Princeton University Press.

Nicolaou, A. I. and McKnight, D. H. (2006). *"Perceived information quality in data exchanges: Effects on risk, trust, and intention to use."* In: Information Systems Research, 17(4), pp. 332–351.

Pashalidis, A. and Mitchell, C. J. (2003). *"A taxonomy of single sign-on systems."* In: Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), pp. 249–264.

Rawlins, B. (2008). *"Give the emperor a mirror: Toward developing a stakeholder measurement of organizational transparency."* In: Journal of Public Relations Research, 21(1), 71-99.

Rigdon, E. E., Ringle, C. M. and Sarstedt, M. (2010). *"Structural modeling of heterogeneous data with partial least squares."* In: Review of Marketing Research, 7(2010), pp. 255–296.

Rogers, E. M. (1995) Diffusion of innovations, Macmillian Publishing Co. doi: citeulike-article-id:126680.

Sarstedt, M., Henseler, J. and Ringle, C. M. (2011). "*Multigroup Analysis in Partial Least Squares (PLS) Path Modeling: Alternative Methods and Empirical Results."* In: Advances in International Marketing, 22(2011), pp. 115–139.

Schau, H. J. and Gilly, M. C. (2003). *"We Are What We Post? Self Presentation in Personal Web*

Schofield, C. B. P. and Joinson, A. N. (2008). *"Privacy, trust, and disclosure online."* In: Psychological aspects of cyberspace: Theory, research, applications., pp. 13–31.

Scott, C. R. (2007). *"Communication and Social Identity Theory: Existing and Potential Connections in Organizational Identification Research."* In: Communication Studies, 58(2), pp. 123–138.

Scott, C., Wynne, D., & Boonthum-Denecke, C. (2016). "*Examining the Privacy of Login Credentials Using Web-Based Single Sign-on-Are We Giving Up Security and Privacy for Convenience?"* In: 2016 Cybersecurity Symposium (CYBERSEC) (pp. 74-79).

SelfKey Whitepaper (2017). URL: https://selfkey.org/wp-content/uploads/2017/11/selfkey-whitepaper-en.pdf (visited on 09/10/2018)

Shrier, D., Wu, W. and Pentland, A. (2016). Blockchain & infrastructure (identity, data security), Massachusetts Institute of Technology. URL: https://cdn.www.getsmarter.com/career- advice/wp-content/uploads/2016/12/mit_blockchain_and_infrastructure_report.pdf. (visited on 23/08/2017)

Sobel, M. E. (1982). *"Asymptotic confidence intervals for indirect effects in structural equation models."* In: Sociological Methodology 1982, 1982, pp. 290–312.

Space." In: Journal of Consumer Research, 30(3), pp. 385–404.

Squicciarini, A., Bhargav-Spantzel, A., Czeskis, A., & Bertino, E. (2006, June). "*Traceable and automatic compliance of privacy policies in federated digital identity management.*" In: International Workshop on Privacy Enhancing Technologies (pp. 78-98). Springer, Berlin, Heidelberg.

Squicciarini, A., Bhargav-Spantzel, A., Czeskis, A., & Bertino, E. (2006). *"Traceable and automatic compliance of privacy policies in federated digital identity management.*" In: International Workshop on Privacy Enhancing Technologies (pp. 78-98). Springer, Berlin, Heidelberg.

Sun, S.-T. and Beznosov, K. (2012). *"The Devil is in the (Implementation) Details: An Empirical Analysis of OAuth SSO Systems."* In: Proceedings of the 2012 ACM conference on Computer and communications security - CCS '12, pp. 378–390.

Suriadi, S., Foo, E. and Jøsang, A. (2009). *"A user-centric federated single sign-on system."* In: Journal of Network and Computer Applications, 32(2), pp. 388–401.

Swann, W. B., Milton, L. P. and Polzer, J. T. (2000). *"Should we create a niche or fall in line? Identity negotiation and small group effectiveness."* In: Journal of personality and social psychology, 79(2), pp. 238–250.

Taddei, S. and Contena, B. (2013). *"Privacy, trust and control: Which relationships with online self-disclosure?"* In: Computers in Human Behavior, 29(3), pp. 821–826.

Taddicken, M. (2014): "The 'Privacy Paradox' in the Social Web: The Impact of Privacy Concerns, Individual Characteristics, and the Perceived Social Relevance on Different Forms of Self-Disclosure" *Journal of Computer-Mediated Communication* 19, pp. 248-273 .

Taylor, S. and Todd, P. (1995). *"Understanding the information technology usage: a test of competing models."* In: Information Systems Research, Vol. 6 No. 2, pp. 144- 76

The Cove Whitepaper (2017). URL: https://coveidentity.com/assets/CoveWhitepaper.pdf (visited on 09/10/2018)

Venkatesh, V. (2000). *"Determinants of perceived ease of use: Integrating control, intrinsic motivation, and emotion into the technology acceptance model".* In: Information systems research, 11(4), pp. 342-365.

Venkatesh, V., Morris, M. G., Davis, G. B., & Davis, F. D. (2003). *"User acceptance of information technology: Toward a unified view."* In: MIS quarterly, pp. 425-478.

VerifyUnion Whitepaper 2018. https://icoinform.com/uploads/pdf/9e1089c29a2bdc3d91584d72662b831d.pdf (visited on 09/10/2018)

Wang, R., Chen, S. and Wang, X. F. (2012). *"Signing me onto your accounts through Facebook and Google: A traffic-guided security study of commercially deployed single-sign-on web services."* In: Proceedings - IEEE Symposium on Security and Privacy, pp. 365–379.

Weber, R. H. (2009). *"Internet of things – Need for a new legal environment?"* In: Computer Law & Security Review, 25(6), pp. 522–527.

Whitbourne, S. and Connolly, L. A. (1999). *"The Developing Self in Midlfe."* In: Willis, S. L. and Reid, J. D. (eds) Life in the Middle: Psychological and Social Development in Middle Age. San Diego, California: Academic Press, pp. 25–45.

World Economic Forum (2011). Personal Data: The Emergence of a New Asset Class. URL: http://www3.weforum.org/docs/WEF_ITTC_PersonalDataNewAsset_Report_2011.pdf. (visited on 23/11/2018)

Zhao, S., Grasmuck, S. and Martin, J. (2008). *"Identity construction on Facebook: Digital empowerment in anchored relationships".* In: Computers in Human Behavior, 24(5), pp. 1816–1836.

Zwattendorfer, B., Tauber, A. and Zefferer, T. (2011). *"A privacy-preserving eID based Single Sign-On solution."* In: Proceedings - 2011 5th International Conference on Network and System Security, NSS 2011, pp. 295–299.

Zyskind, G., Nathan, O. and Pentland, A. S. (2015). *"Decentralizing privacy: Using blockchain to protect personal data."* In: Proceedings - 2015 IEEE Security and Privacy Workshops, SPW 2015, pp. 180–184.