European Journal of Information Systems (2014) 23, 36–50

www.palgrave-journals.com/ejis/

EMPIRICAL RESEARCH

Users' willingness to pay for web identity management systems

Heiko Roßnagel[1], Jan Zibuschka[1], Oliver Hinz[2] and Jan Muntermann[3]

[1]*Fraunhofer-Institute for Industrial Engineering IAO, Stuttgart, Germany;* [2]*TU Darmstadt, Germany;* [3]*University of Göttingen, Göttingen, Germany*

Correspondence: Heiko Roßnagel, Identity Management, Fraunhofer-Institute for Industrial Engineering IAO, Nobelstr. 12, 70569 Stuttgart, Germany.
Tel: +49 71 1970 2145;
Fax: +49 71 1970 2401;
E-mail: heiko.rossnagel@iao.fraunhofer.de

Abstract
Electronic services such as virtual communities or electronic commerce demand user authentication. Several more or less successful federated identity management systems have emerged to support authentication across diverse service domains in recent years. In this paper, we explore the determinants for success and failure of such systems with a focus on Germany representing one of the largest markets in Europe. To achieve this goal, we analyze the preferences and willingness to pay of prospective users by conducting a choice-based conjoint analysis. Our results indicate that users prefer simple systems where an intermediary takes care of their data. An additional market analyses confirms these findings and contradicts the assumptions of many researchers, especially in the fields of engineering and computer science, supporting systems with higher and higher levels of privacy and security.
European Journal of Information Systems (2014) **23,** 36–50. doi:10.1057/ejis.2013.33; published online 19 November 2013

Keywords: federated identity management; identity management systems; choice-based conjoint; electronic commerce

Introduction

Reliable authentication is one of the basic requirements of e-commerce and other transaction services on the web (Schläger *et al*, 2006). So far, passwords have been the predominant authentication method. Passwords are easy to use and do not require expensive hardware or software on the client side (Mannan & Van Oorschot, 2007). On the other hand, the use of passwords leads to several problems, such as inconvenient password management issues (Recordon & Reed, 2006), password reuse (Ives *et al*, 2004), and other security problems (Neumann, 1994). Federated identity management (FIM) has emerged as a promising technology for authenticating users and distributing identity information across security domains (Maler & Reed, 2008). To give a concise definition: *Federated identity management (FIM) provides a way to share user authentication information across a variety of domains* (Landau & Moore, 2011). It offers the promise of a single sign-on for different domains and service providers by providing a unified authentication and authorization infrastructure that eliminates the need for passwords. This includes, for example, public key infrastructure (PKI) and contemporary identity provider systems, but does not include password-based systems, which are of course still relevant as the incumbent technology.

Several different solutions for FIM have been introduced over the last few years, some of them backed by large companies such as Microsoft or IBM. The success of these systems has been mixed. Some systems, such as Microsoft Passport, have not been successful and have been replaced

Received: 21 January 2011
Revised: 15 July 2011
2nd Revision: 06 February 2012
3rd Revision: 10 September 2012
4th Revision: 19 September 2013
Accepted: 30 September 2013

(Whitley & Hosein, 2008). Other systems have been highly successful in particular specialized domains, such as SAML in e-business scenarios (Hühnlein *et al*, 2010). In other domains, however, the same systems have not achieved this kind of success. Their mixed success has been attributed by researchers to various factors, including security and privacy shortcomings (Kormann & Rubin, 2000; Hansen *et al*, 2004), as well as usability issues (Dhamija & Dusseault, 2008). This research has a strong focus on the supply side of FIM. However, to our knowledge, there has only been very little empirical work done to corroborate these claims from a demand perspective. We aim to close this gap with this contribution. This study focuses on individuals' willingness to pay (WTP) for the use of FIM, as this is the prevailing revenue scheme for commercial deployments of identity management, as has been shown by studies investigating, for example, the German electronic signature market (Roßnagel & Lippmann, 2005), but alternative revenue schemes – which are out of the scope of this paper – are also possible, for example, website operators might pay the FIM provider.

We conduct a choice-based conjoint (CBC) analysis to determine prospective users' preferences. On the basis of a representative sample of the German Internet population, we measure the impact of various aspects of the design of FIM solutions on users' WTP.

The remainder of this paper is structured as follows. We first present a review of the related literature. Then, we describe the methodology of our approach and present the study design. The next section presents the empirical results of our micro-level analysis of market demand. We then compare these results with the actual market success of selected FIM solutions in the following section, as a mixed-method approach acknowledging that we did only survey one side of a multi-sided market. The implications of our results are discussed before we summarize our findings.

Related work

There have been several surveys of web identity management solutions, including both in-depth reviews of available technologies (Lopez *et al*, 2004) and generalized taxonomies (De Clerq, 2002), using various definitions of the term 'identity management'. As stated above, we define FIM according to Landau & Moore (2011) as *a way to share user authentication information across a variety of domains*. FIM enables websites to offer cross-domain single sign-on to users (Maler & Reed, 2008). Several factors affecting the success of such systems in the market have been discussed in the literature:

1. Numerous authors have identified the level of *privacy* that such a system can offer to users as a key factor (Hansen *et al*, 2004; Jøsang *et al*, 2007; Acquisti, 2008). For example, Hansen *et al* (2004) propose 'privacy-enhancing identity management' and call for identity management systems that offer maximal technical privacy guarantees and thus may minimize the trust required to use such a system. 'User-centric identity management', which provides users full control over their personal information, is often used as a basis for the optimal design of such systems. These authors also argue that improving privacy will address the problem of lacking trust, which is seen as a major inhibitor of the success of identity management systems.
2. Research has identified *security* as another important success factor for identity management (Dhamija & Dusseault, 2008; Krolo *et al*, 2009). For instance, Kormann & Rubin (2000) identify a weakness in Passport that is widely perceived (Fu *et al*, 2001) as having led to the demise of the system by undermining its users' trust. Dhamija & Dusseault (2008) identify security issues as one of the most pressing problems of identity management today, but also point out that it is critical to design systems that are both secure and easy to use.
3. This leads us to the next critical success factor often listed in the literature: *usability* (Jøsang *et al*, 2007; Dhamija & Dusseault, 2008). The consensus is that because identity management systems are so complex (due to privacy and security requirements), it is very difficult to design a comfortable user interface, and such an interface would at the very least have to be fundamentally different from current interfaces. In addition, usable systems may coax users into revealing their personal information more readily (Dhamija & Dusseault, 2008).
4. Finally, the *interoperability* of identity management systems has been discussed as a critical success factor (Backhouse *et al*, 2003; Bhatti *et al*, 2007); a system's interoperability determines the breadth of its possible application areas, which in turn influences its usefulness for the client.

Although these factors do not constitute a complete list, research has identified them as the most important factors and we will focus on them in this paper. Whereas most research has discussed single success factors in isolation, there are several related studies that have investigated the diffusion of FIM systems, such as Hühnlein *et al* (2010), who take a qualitative approach. Acquisti (2008) discusses the economic facets of privacy in identity management, focusing on the role and benefits of price discrimination (Hinz *et al*, 2011) and how it interacts with privacy. Zibuschka & Roßnagel (2008) describe the network effects arising from distributed single sign-on architectures where the utility for users increases as more services implement protocols that are compatible with the system that they use. A recent study performed by the European Commission, labeled 'the largest survey ever conducted regarding citizen's behaviours and attitudes concerning identity management, data protection and privacy' (European Commission, 2011), investigated broadly non-technological factors contributing to users' privacy attitudes. The study explores the related questions of whether the users see disclosing personal information as part of modern life,

what information they are willing to disclose, or whether they read e-commerce services' privacy policies. According to the study, 74% of Europeans see disclosing personal information as a part of modern life, where personal information includes financial information. This tendency is strongest for the younger generation of 'digital natives'. These findings match the results of another recent survey by BITKOM, a German association for information technology representing more than 1600 companies (BITKOM, 2011).

Another recent contribution (Landau & Moore, 2011) investigated current trends in FIM, specifically adoption by relying parties and usage, both complimentary indicators to the user preference we measure in this contribution. Their study is based on statistics published by Alexa, and shows Facebook as the leading FIM system both in terms of adoption by relying parties (34.9%) and in terms of usage (40.52%), followed by Google in second place. They also provide cases, in which stakeholder incentives may be conflicting, which they call 'economic tussles'. These conflicts are matched with possible use cases of FIM, showing that the 'tussles' are applicable to most of the use cases they selected.

In the study most relevant to our work, Mueller *et al* (2006) examine user preferences and WTP for FIM systems in South Korea using seven different attributes of digital identifiers. With regard to privacy and security, they use the generic attributes 'security level' (ranging from 'completely public' to 'completely secure') and 'private information' (ranging from 'name and email' to 'social security number and credit card information'). The success factors affecting interoperability are identified as the 'industry sector' and 'coverage of identifier'. Usability was not addressed at all. Instead, the researchers used the 'service provider' attribute to evaluate brand effects, a dummy variable for switching to an alternative identifier to estimate switching costs and the monthly costs of the product. Their results show that security is highly regarded, with 91% of the population preferring the 'completely secure' option. Furthermore, there seems to be a huge gap between WTP for 'complete security' (US$5.65) and WTP for the next best option, 'very secure' ($0.812), which is defined as a system that reveals private information in response to legal requests but is otherwise secure. We believe that the use of this attribute can be misleading. Studies have shown that users often claim in surveys to value security and privacy but actually do not act accordingly, demonstrating a discrepancy between attitudes toward privacy and security and actual behavior (Greenwald *et al*, 2004; Shostack & Syverson, 2004; Berendt *et al*, 2005). Given that even the authors admit that a 'completely secure' system is hypothetical and cannot be achieved in practice, we believe that it is inappropriate to include this attribute in our study. With regard to privacy, Mueller *et al*'s (2006) results show that users prefer to withhold their most sensitive private information. However, the price that they are willing to pay for privacy is lower than initially expected by the authors. Mueller *et al* (2006) speculate that this dynamic might be unique to South Korea and that surveys of other populations in different cultures may produce different results. Not surprisingly, the attribute 'coverage of identifier' turned out to be a critical success factor reflecting the power of network effects. In contrast, the attribute 'service provider' did not play an important role.

Our goals extend beyond the work of Mueller *et al* (2006) in three respects: (1) because we focus on Germany, one of the largest European markets, we can expect cultural differences between the two studies, for example, in terms of the respondents' preferences, and thus potentially different outcomes;[1] (2) the identity management market has evolved dynamically in the last 5 years, with new technologies and application areas moving into the spotlight; we focus in this study on FIM systems for the Web (Hühnlein *et al*, 2010; Maler & Reed, 2008), a market that is less heavily regulated than related markets (Hühnlein *et al*, 2010), and thus allows for a more direct comparison of user preferences to events in the market; and (3) to ensure that our results are applicable to identity management system design, we focus on characteristics that could be applied during the early stages of information system development (Chapman *et al*, 2008), specifically for feasibility analyses (Barker *et al*, 2007) that can be performed before deployment costs are sunk, as opposed to properties of deployment. Overly generic attributes (such as 'security level' cited by Mueller *et al*, 2006) are not suitable in this context. On the other hand, overly specific properties of concrete system implementations, such as user interfaces for specific tasks and associated usability factors, are also not within the scope of this study. Whitley (2012) discusses this in some detail and also points out that: *Achieving close to 100% certainty in a unique identity is always a costly process, particularly because of the opportunities for fraud that are opened up if an unique identity is incorrectly assigned*, illustrating that while consumers aim for complete assurance the level of assurance cannot be guaranteed even by technologies that are nearly completely secure or privacy-friendly from a technological standpoint, as, for example, *most public services still use 'names' as important (secondary) identifiers for the citizens they interact with* (Whitley, 2012), enabling a high level of linkability even using technologies enabling anonymous identity disclosure.

Research methodology

Methodology

User preferences are central to the success of new products. They can also be relevant even in heavily regulated markets, where they can serve as guiding information for steering regulation. We therefore conduct a choice experiment and determine prospective users' preferences and

[1]Because of the different study setup, the reasons for which are given in (2) and (3), we cannot directly compare our results with those of Mueller and colleagues. Our findings only represent the German case.

WTP for different FIM solutions. By focusing on WTP, we can easily compare different FIM designs and express the prospective users' preferences in a single dimension.

We use a CBC analysis to elicit choice behavior and then use this data to estimate partworths using the Hierarchical Bayes (HB) method, which we then transform into the WTP space. In a second step, we cluster prospective consumers into segments according to their psychographics. The results of this analysis on a micro level allow us to determine what is really important for prospective users of FIM systems. This is very useful information for all suppliers in this domain. In a second step, we validate our results based on this micro-level analysis and use these insights to explain the success or failure of present FIM systems.

CBC and WTP estimation In operational research and marketing, models have been developed for selecting optimal products and determining profit-maximizing pricing strategies (e.g., Kohli & Krishnamurti, 1989; Day & Venkataramanan, 2006). Many of these models use estimates of consumer preferences and WTP, which is the price point at which a consumer becomes indifferent as to the choice between purchasing or not purchasing a product. This information can be derived through conjoint analysis.

CBC analysis is frequently used because of its greater task similarity between choices and market behavior (Natter & Feurstein, 2002). Moreover, several studies indicate that CBC analysis performs better than rating-based conjoint analysis (Karniouchina *et al*, 2009). We therefore use CBC to determine the partworths utilities for different features of FIM solutions. By using CBC, we can estimate the attribute-based partworths, the price parameter, and the parameter for the no-purchase option:

$$P_{h,i} = \frac{\exp(u_{h,i})}{\exp(u_{h,NP}) + \sum_{i' \in C_a} \exp(u_{h,i'})} \quad (h \in H, i \in I)$$

where $P_{h,i}$: probability that consumer h chooses product i; $u_{h,i}$: utility of product i for consumer h; $u_{h,NP}$: utility of no-purchase option for consumer h; C_a: index set of alternatives in choice set a ($C_a \subseteq I$); H: index set of consumers; I: index set of products (not including the no-purchase option).

The probability that a customer will choose a product depends on the utility of product i for consumer h, $u_{h,i}$, which is equal to the sum of the attribute-based partworths and the partworth of the price:

$$u_{h,i} = \sum_{j \in J} \sum_{m \in M} \beta_{h,j,m} \cdot x_{i,j,m} + \beta_{h,price} \cdot p_i \quad \text{with} (h \in H, i \in I)$$

where $\beta_{h,j,m}$: parameter of level m of attribute j for consumer h (attribute-based partworth); $x_{i,j,m}$: variable indicating whether product i features level m of attribute j; $\beta_{h,price}$: price parameter for consumer h; p_i: price of product i; M: index set of levels; J: index set of attributes without price.

We estimate the parameters for consumers in H using the HB model. The HB model has two levels. First, at the higher level, it is assumed that consumers' partworths are described by a multivariate normal distribution. Such a distribution is characterized by a vector of means and a matrix of covariances. Then at the lower level, it is assumed that given a consumer's partworths, his or her probability of choosing particular alternatives is governed by a multinomial logit model. HB has the advantage of allowing for the flexible incorporation of prior information about model parameters. Moreover, HB allows the estimation of individual-specific estimates and it can account for uncertainty in these estimates. We specially chose HB because it allows us to estimate partworths on the individual level and does not require a large number of responses. For more information on HB, we refer to Gelman *et al* (2004). By using CBC and HB, we end up with individual partworths for the different features of FIM solutions. In our next step, we transform the partworths into monetary values.

We define a consumer's $WTP_{h,i}$ for a product as the price at which consumer h is indifferent as to whether s/he purchases or does not purchase product i (Moorthy *et al*, 1997). The utility of the product then equals the utility of not purchasing it, or $u_{h,NP}$. The latter is equal to the value of the no-purchase option $\beta_{h,NP}$:

$$\sum_{j \in J} \sum_{m \in M} \beta_{h,j,m} \cdot x_{i,j,m} + \beta_{h,price} \cdot WTP_{h,i} = \beta_{h,NP}$$

Rewriting this equation leads to:

$$WTP_{h,i} = \frac{1}{\beta_{h,price}} \cdot \left(\beta_{h,NP} - \sum_{j \in J} \sum_{m \in M} \beta_{h,j,m} \cdot x_{i,j,m} \right)$$

According to economic theory, consumers maximize their consumer surplus and thus choose the product in the choice set that generates the highest consumer surplus. If the prices of all products are higher than a consumer's WTP, the consumer selects the no-purchase option. By applying this concept, we can calculate the WTP for every product i for every consumer h. This method also allows us to extrapolate WTPs that are beyond the range of the price levels mentioned.

Clustering and market performance In a third step, we use cluster analysis to identify different market segments. We use information about consumer mindsets for clustering. We expect characteristics like risk-taking, trust, and price consciousness to determine the different segments. We first use single-linkage clustering to determine the optimal number of segments. This helps us to identify outliers, which are eliminated at this stage before we estimate the final clusters using Ward's (1963) linkage method.

This analysis yields the WTP for different segments and allows us to determine the best products for these different segments. Furthermore, these results allow us to explain the success or failure of present FIM systems. In our last

step, we thereby use our micro-level findings to cross-validate the development of the FIM market and thus examine the macro level.

Study design

CBC design We conduct a choice experiment by presenting different choice sets including a no-purchase option. The choice sets consist of two different product alternatives and the no-purchase option. One critical success factor in conjoint analyses is the choice of which attributes to include in the survey questionnaires (Auty, 1995). Therefore, we conducted a pre-study with 216 respondents (not representative for the internet population) in early 2010 to determine the most relevant attributes. For this pre-study, we used all attributes included in Mueller *et al* (2006) except 'security level', which we replaced with several attributes that focused on security- and privacy-relevant system properties (e.g., authentication method, access control, identity certification, anonymity). We also included the attribute 'application area' as a possible alternative to 'industry sector' and 'coverage of identifier'. We tested price levels from €1 annually to €20 annually. We found that a significant amount of subjects had a higher WTP than €20, and thus we increased the price level range in the main study. We further examined the partworths and calculated the individual WTP using HB (see previous section). The prediction accuracy measured by the first choice hit rate (HR) was 77%, which is much higher than the 33% chance criterion. The internal HR for the pre-study was 87%, which is excellent. On the basis of the calculated partworths for the attributes in our pre-study, we used the following three attributes with the highest importance along with price as a fourth attribute:

The first attribute is the *level of identity certification* provided, which relates directly to the *security* success factor as identified in the literature; it can serve as a tangible indicator for users looking to make a quick security assessment. Solutions that certify the identity of their users or even provide legally binding identification should be perceived as more secure than those that rely only on user claims. Higher levels of certification are also usually accompanied by stronger authentication based on smartcards or biometry, for example, which further links them to the security level of the overall system. In our pre-study, authentication factors and certification were the highest-rated security attributes but were perceived as far less relevant than application area, for example. Thus, it made sense for us to merge those factors. The resulting attribute should be relevant to users and still meaningful to system designers. We consider three different levels for this attribute:

(1) *User claim-based identification*, which implies that the relying party only has access to unverified, self-asserted claims provided by the users concerning their identity attributes.
(2) *Certified identification,* in which an identity provider certifies the identities of its users. Falsely certified identities will not *per se* result in liability of the operator of the system.
(3) *Legally binding identification*, indicating that the identification is strong enough to be enforceable if disputes arise in resulting transactions. Under German law (SigG §17 (1)), this requires secure *Signaturerstellungseinheiten* (signature creation units), such as electronic signature cards, for example the national German eID. The operator of the system may be held liable for falsely certified identities if he is responsible for the error.

As the literature has identified privacy as a key success factor, the second attribute of interest is the *level of privacy protection* provided. With regard to privacy, users seem to care most about how much information has to be supplied to identity management providers and where it will be processed. The privacy attribute presents architectural choices by system designers and their impact on the amount of identity information, location where this information is stored, and the entity that controls it. For example, the identity provider might act as an information intermediary for identity information (Bakos, 1991), which would have significant privacy implications. As Wohlgemuth & Müller (2006) put it: *Privacy in business processes with proxies is not possible.* As with security, those attributes are perceived as less relevant than application area but as significantly more relevant than industry sector, as proposed by Mueller *et al* (2006) according to our pre-study. Again, we consider three different scenarios:

(1) *Intermediary governs the data:* Here, the identity provider stores (and potentially controls) all relevant user data and disclosure of this data to relying parties is controlled via policies on the identity provider's side.
(2) *User governs the data*: Here, users' identity information is governed by and its disclosure is under the exclusive control of users. Identity information is provided by the user to the relying party and stored on the user's client. The user may have to interact with a third party to acquire a valid credential in advance.
(3) *Anonymous credentials*: Here, all user transactions are unlinkable (Camenisch & van Herreweghen, 2002). A relying party only receives the information disclosed to it, and cannot recognize repeat visitors unless a combination of attributes providing a positive identification has been disclosed (multi-show unlinkability). Some of these systems even provide multi-show unlinkability *vs* the party creating the (original) anonymous credentials (Camenisch & van Herreweghen, 2002).

We assume that the *application area* influences consumer behavior as a result of solution interoperability and therefore generate three different attribute levels that incrementally offer more application options. Application area was the most important attribute for those who

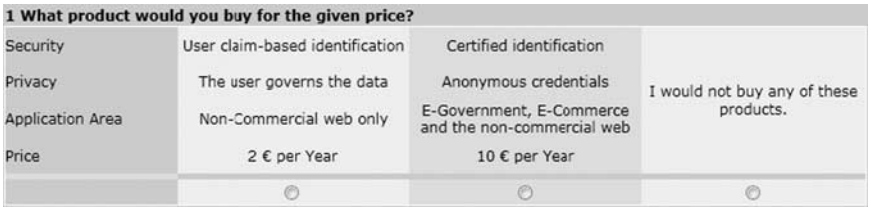

Figure 1 Example of choice set.[2]

Table 1 Attributes and attributes levels in CBC

Attributes	*Attribute levels*
Security	● User claim-based identification ● Certified identification ● Legally binding identification
Privacy	● Intermediary governs the data ● User governs the data ● Anonymous credentials
Application area	● Non-commercial web only certified identification ● E-Commerce and the non-commercial web ● E-government, e-commerce, and the non-commercial web
Price	● €2 annually ● €5 annually ● €10 annually ● €20 annually ● €40 annually

completed our pre-study and was perceived as more relevant than 'coverage of identifier' or 'service provider' used by Mueller *et al* (2006). At the same time, the attribute levels given here have clear implications for the design of identity management systems, and rather different architectures have emerged in each application area. Thus, attributes should once again be relevant for users and meaningful for system designers.

(1) *Non-commercial web only*: For example, for social networks and gaming platforms.
(2) *E-commerce and the non-commercial web*
(3) *E-government, e-commerce, and the non-commercial web*

As usability depends on the specific implementations of identity management solutions and because FIM solutions can be considered experience goods, we do not include this attribute in our analysis. As we aim to examine user WTP, and because FIM providers going beyond the basic configuration (1-1-1) usually charge fees for their services (Roßnagel & Lippmann, 2005), we test five different price levels that are commonly used in the market: €2 annually, €5 annually, €10 annually, €20 annually, and €40 annually. These price levels cover the high prices observed by Roßnagel & Lippmann (2005) for systems that provide legally binding identification in the German market, as well as price reductions that might be possible due to lower levels of security or future economies of scale (Table 1).

The attribute levels for the product alternatives are systematically varied by creating an efficient design. We applied a D-efficient fractional factorial design. A major challenge is the creation of an efficient choice design (Street & Burgess, 2007). For this purpose, we used Sawtooth Software to construct a D-optimal (3^3●5) factorial design with 16 choice sets. These designs are known for their high efficiency and their suitability for a diverse range of research designs. Each choice set shows two different alternatives and a non-purchase option. We assume that a user does not choose more than one FIM. This assumption is not very strong as a user must pay the annually fee multiple times if she or he wants multiple FIM solutions for different usage situations.

Using online software provided by Burgess (2007), we find that the efficiency compared with optimal design is 91.29%. The observations from 14 of 16 choice sets are included in the estimation and the remaining two choice sets are used to test the predictive validity. See Figure 1 for an example choice set.

Conjoint analysis in general creates hypothetical situations for prospective consumers that can lead to a hypothetical bias. For example, this bias can result from strategic behavior of respondents hoping to get a product or service for less in the future based on their own input. This phenomenon has been reported in a number of studies (see, e.g., Cummings & Taylor, 1999). Eliciting consumers' true WTP is not trivial; WTP is an unobservable construct. Recent insights based on real purchases show that CBC does indeed generate hypothetical biases but still leads to the right demand curves and the right pricing decisions (Miller *et al*, 2011). These results may be the reason for the success of CBC in business practices.

Latent constructs We also gather demographic information like age, family status, income, gender, and information about consumer mindset. This psychographic information is then used to determine different user segments via cluster analysis (Punj & Stewart, 1983; Green & Krieger, 1991; Krieger & Green, 1996). We use well-established scales from information systems research, marketing, and psychology. We hypothesize that trust will have an influence on user WTP. People who have

[2]Translated from German.

trust in others are less likely to pay for security systems like FIM systems than are people who are distrustful. We use the trust scale from the NEO Personality Inventory (Costa & McCrae, 1992). As Wu and Ayalagaytan (2013) have shown that WTP in online markets depends on buyers' risk attitudes, we also assume that risk-takers have a lower WTP and therefore include the risk-taking scale from the Jackson Personality Inventory (Jackson, 1994). We also include scales for extravagance (Cloninger, 1994) because people with high scores on this scale typically want to be unique and differ regarding their adoption of new technologies. Generous people generally have a higher WTP (Haeusel, 2000), whereas price consciousness (Lichtenstein *et al*, 1993) is likely to have a negative influence on prospective users' WTP. The survey also includes questions regarding opinion leadership (Childers, 1986). This allows us to evaluate the attitude of opinion leaders regarding FIM, which is of particular importance to the diffusion process for this new technology. We further include the adventurousness scale from the NEO Personality Inventory (Costa & McCrae, 1992) as we assume that people who are adventurous are more likely to try out new products but on the other side may have a lower WTP for technologies that eliminate risks. All scales are measured using items on a 7-point Likert scale and detailed information on the used items can be found in the Online Appendix.

We use this information to determine different segments of prospective users based on cluster analyses and to examine the differences between the segments in terms of user preferences for different FIM solutions.

Empirical results

We designed the study and a leading German market research firm acquired a representative sample for our study in late 2010, which led to a response rate of 100%. The respondents had to complete an online questionnaire and were identified by a unique ID. Respondents were only remunerated if they completed the questionnaire in a sensible manner; repeated aberrant response behavior can also lead to an exclusion from the sample for further studies. Nevertheless, we carried out the following validity checks: time to complete, response style agreement, extreme response style, and neutral response style for the latent constructs measured with Likert scales. We did not observe any apparent aberrant response behavior with respect to the psychographic and demographic items. The response behavior with respect to the choice experiment is analyzed later. Interviewing such a sample is costly, but this approach usually leads to high-quality answers.

Demographics

We have obtained a rather representative sample of the German Internet population if non-adults are excluded, with $n = 249$ completes. The respondents' average age is about 41 years (mean of the German Internet population according to ARD; ZDF (2010) is 40.65 years) with a standard deviation of 11.5 years and a minimum of 18 years and maximum of 64 years. Of the respondents, 141 (56.6%) are male, whereas 108 are female (43.4%). This proportion is consistent with the numbers reported in large-scale studies (male: 54.3%, female: 45.7%). The average household size is 2.5, and the majority of these individuals are married (45.8%) or living with a partner (28.5%). The mean number of credit cards is 1.95 (standard deviation 0.89).

About 15% of the sample is composed of students or trainees, whereas the majority (~55.4%) is employees and 18.1% are retired or unemployed. This perfectly reflects the German Internet population according to previous large-scale studies. Approximately 50% received their diplomas from German secondary school and qualified for university admission. A total of 74 respondents graduated from a university or university of applied sciences.

Psychographics

We compute the Cronbach's α for the factors related to respondent mindset and compare them with the values reported in the study in which the particular scale was originally developed. This allows us to assess the validity and reliability of the scales (Table 2).

The Cronbach's α's in our study are similar to the values reported in the original studies and are above the recommended reliability threshold of 0.7 in all cases. We also conducted explorative factor analysis with Varimax rotation with SPSS and identified seven components reflecting our latent constructs. We conclude that the items in the survey can be used to describe the latent constructs and use the average scores for the particular items as construct score for further analysis (Table 3).

CBC results

We use HB estimates and standard diffuse priors. The reported results are obtained using 20,000 iterations that we retain after discarding the initial 40,000 iterations (=60,000 iterations in total). We assess convergence according to the trace plot of the likelihood and parameters.

We evaluate the validity of the CBC by computing the (internal) HR and the mean absolute deviation (MAD) (Brazell *et al*, 2006) for the 14 choice sets and the (predictive) HR and MAD in the two holdouts. We used the parameter estimates to calculate the first-choice HR in the 16 choice sets as a measure for the internal validity. The first-choice HR measures the frequency with which CBC predicts the same first-ranked as observed. The two holdouts were used as a measure for the predictive validity.

The internal HR is excellent at 93%, and the internal MAD is 10.74%, whereas the predictive HR is also excellent at 88.2% (the predictive MAD is 13.8%). These results are significantly higher than the one-third chance criterion. The CBC results provide further face validity: 21 respondents never select the no-purchase option, whereas 139 respondents always select the no-purchase option. In other words, even with a fee as low as €2 per year, 55.8%

Table 2 Cronbach's α in original studies and in our study

Latent construct	*Cronbach's α in this study*	*Cronbach's α reported in original study*	*Original study introducing latent construct*
Extravagance	0.79	0.85	Cloninger (1994)
Price consciousness	0.85	0.84	Lichtenstein *et al* (1993)
Opinion leadership	0.95	0.79	Childers (1986)
Generosity	0.82	0.67	Haeusel (2000)
Risk-taking	0.72	0.78	Jackson (1994)
Trust	0.80	0.82	Costa & McCrae (1992)
Adventurousness	0.73	0.77	Costa & McCrae (1992)

Table 3 Average scores of latent constructs in our study

Latent construct	*Average score*
Extravagance	5.5
Price consciousness	2.9
Opinion leadership	4.0
Generosity	3.6
Risk-taking	5.3
Trust	3.7
Adventurousness	3.5

of our representative sample does not envision entering the market at all. These respondents do not seem to see any benefits of FIM.

We further investigate this interesting fact by estimating a logistic regression to examine what types of respondents are not in the market. The dependent variable is *neverChoice* (0 or 1), and we use demographics and psychographics to explain what types of individuals are not interested in FIM at all. We indicate this by always selecting the no-purchase option. The estimation yields a Nagelkerke's R^2 of 16.5%. We observe that people who are very price conscious are not willing to adopt this new technology ($P<0.1$). This seems reasonable. People who are willing to take high risks are also more likely not to be in the market for FIM systems ($P<0.05$). Or the other way round: risk-averse people are more likely to adopt FIM solutions. This is in line with the findings of Wu and Ayalagaytan (2013), who have shown that risk attitude influences WTP in online markets. Another interesting finding is that people with a high number of credit cards are more likely to adopt FIM systems ($P<0.05$). As we control for income (which has no significant influence), we assume that people with a high number of credit cards are more active on the internet and would thus value FIM solutions more than the average customer. According to Liebermann & Stashevsky (2002), one of the main perceived risks that form barriers to web usage is the threat of losing credit card information (Table 4).

Table 4 Logistic regression with 'out of the market' as the dependent variable

	Regression coefficient	*Standard error*	*z*	*Significance*
Constant**	−2.823	1.313	−2.15	0.032
Price consciousness*	0.218	0.130	1.68	0.094
Opinion leadership	0.075	0.096	0.78	0.437
Risk-taking**	0.305	0.131	2.33	0.020
Trust	0.082	0.118	0.70	0.486
Extravagance**	0.210	0.089	2.36	0.018
Generosity	0.117	0.137	0.85	0.394
Adventurousness	−0.076	0.147	−0.52	0.605
Age	0.010	0.013	0.74	0.460
Gender (0: male /1: female)	−0.201	0.302	−0.67	0.506
Household size	−0.176	0.111	−1.58	0.115
Net Income	0.043	0.055	0.78	0.433
Number of credit cards**	−0.425	0.178	−2.39	0.017

Note: *: $P<0.1$; **: $P<0.05$.

A similar logistic regression used to explain why some never select the no-purchase option (dependent variable: *alwaysChoice*) yields a Nagelkerke's R^2 of 18.3%. We find that people who are risk-averse ($P<0.1$) or have a low score on the adventurousness scale ($P<0.05$) are more likely to always select an FIM product in the CBC analysis and thus are promising prospective users of FIM solutions.

As suggested by Gensler *et al* (2012), we exclude the respondents who always or never select the no-purchase option from further analysis because the estimates for WTP cannot be computed reliably.

Clustering

On the basis of the representative sample of individuals in the market for FIM solutions, we isolate different segments using the single-linkage clustering approach to analyze the mindset of the assessed consumers (in terms of risk-taking, trust, price consciousness, etc.). We find that using four segments appears to be most appropriate. We observe the following segment characteristics (Table 5).

The first segment is rather risk-averse and not very adventurous. We therefore call this segment 'the risk-averse' segment. It consists of more female than male users having a net income above average. The second segment, which includes 28 individuals (more males than females), is referred to as 'the pioneers' because of its very high score on the opinion leadership scale. It is also very risk-taking and adventurous; these are usual characteristics of opinion leaders. The net income is below average. The third segment is quite the opposite, with a low score on the opinion leadership and extravagance scale. This segment, however, is not very price-conscious, which might indicate high WTP for products that have been proven to be beneficial for early adopters. We call this segment 'the

Table 5 Segment characteristics

Consumer segment	*Extravagance*	*Price consciousness*	*Opinion leadership*	*Generosity*	*Risk-taking*	*Trust*	*Adventurousness*
1 ($n=21$)	5.31	3.00	3.01	3.16	3.55	3.98	2.48
2 ($n=28$)	5.64	2.11	4.50	4.15	5.86	4.20	4.10
3 ($n=16$)	4.41	1.92	2.01	2.90	5.64	2.85	3.06
4 ($n=24$)	5.73	4.13	4.38	3.13	5.14	3.46	3.85
Average	5.37	2.83	3.68	3.42	5.08	3.71	3.46

followers'. The last segment is rather average on most of the scales; we therefore call that segment 'the average users'. Like the third segment, the fourth segment also consists of about the same number of male and female users.

Preferred products and WTP

On the basis of the calculated utility levels, it is possible to assess the different segments' WTP for products with various attribute combinations.

For each consumer segment, we assessed the three best product alternatives by determining the attribute combinations that enjoy the highest WTP. Given the best product alternatives for the four segments, significant WTP differences can be observed between these segments. With a maximum of €48.70, risk-averse consumers show the highest WTP: that is, FIM systems that provide risk mitigation functionalities appear very valuable to this segment. For this segment, legally binding identification and e-commerce and non-commercial web use represent the most relevant product features. In contrast, the level of privacy protection plays a minor role here; the three best product alternatives only vary with regard to this attribute. On the other hand, the pioneers are willing to spend a maximum of €12.16 for their best preferred product alternative only. For this opinion-leading segment, the most important product attribute appears to be anonymous credentials – a feature that is widely discussed in academia (Camenisch & Van Herreweghen, 2002; Tsang *et al*, 2007). This interest in anonymous credentials could be a result of the German 'informationelle Selbstbestimmung' approach to privacy, which is based on the individual's right to self-determination with regard to their personal information (Hornung & Schnabel, 2009). It is noteworthy that the pioneers do not vote for identity claims exclusively provided by the user herself or himself. Furthermore, this segment prefers more application areas to be available, including e-government. As the pioneers seem to be price sensitive, it might be beneficial for FIM providers to apply a price penetration strategy where the price for the service is rather low at the beginning. This would attract the pioneers, and when the diffusion starts to accelerate the prices could be raised as the followers show a remarkable maximum WTP of €35.95. The followers exhibit a strong preference for certified identification and do not prefer anonymous credentials, but they do prefer that the technology have more application areas. Finally, the average users report an average maximum WTP of €23.85 and clearly prefer certified identification and the largest number of application areas possible. Unlike for the followers, privacy protection only plays a minor role for the average users and affects WTP very little.

If product differentiation is not desirable or possible and a firm would create just one product, we analyze the preference of the entire sample (last row in Table 6). For the overall sample, which features an average maximum WTP of €18.10, both certified identification and flexible application (including e-government) are the product attributes of choice. In contrast, privacy protection appears to play a minor role only, and user-governed data is least preferred. For the overall sample, certified identification, intermediary governed data, and the most flexible application areas represent the most favored product alternatives.

For the three attributes explored, we can conclude the following. Certified identification is the preferred security option, and only risk-averse consumers prefer legally binding identification. User claim-based identification does not appear to be a valid option; it is not listed for any of the three best product alternatives. With regard to privacy protection, there is no clear common preference. However, intermediary-governed data solutions and anonymous credentials are most favored, whereas user-governed data solutions appear less favored. Users clearly prefer FIM use to be as flexible as possible. Most user segments (all except the risk-averse) prefer the technology to have as many areas of application as possible and particularly that it supports e-government use; non-commercial web use only does not appear to be a reasonable option.

Market performance of contemporary FIM systems

To complement our quantitative survey of one side of a multi-sided market, we now examine the performance of the leading FIM systems in the market and illustrate parallels between the developments in the market and our results as presented in the previous section. The systems considered in this section are Microsoft CardSpace (Cameron & Jones, 2007), which represents the credentials-based approach; OpenID (Recordon & Reed, 2006), a URL-centric initiative from the Web 2.0 domain; and the recent initiative by the leading online community site Facebook.

Table 6 WTPs of preferred product

Consumer segment	*Name*	*1. Best product (a, b, c) (WTP)*	*2. Best product (a, b, c) (WTP)*	*3. Best product (a, b, c) (WTP)*
1 ($n=21$)	Risk-averse	3-1-2 €47.80	3-3-2 €46.01	3-2-2 €43.83
2 ($n=28$)	Pioneers	2-3-3 €12.16	3-3-3 €10.95	2-3-2 €9.71
3 ($n=16$)	Followers	2-1-3 €35.95	2-2-3 €31.79	2-1-2 €29.86
4 ($n=24$)	Average users	2-3-3 €23.85	2-1-3 €23.42	2-2-3 €21.26
Total ($n=89$)	Entire sample	2-1-3 €18.10	2-3-3 €17.59	2-2-3 €16.30

Notes: With the attribute combinations (a, b, c): $a=1$: User claim-based identification; $a=2$: Certified identification; $a=3$: Legally binding identification; $b=1$: Intermediary governs data; $b=2$: User governs data; $b=3$: Anonymous credentials; $c=1$: Non-commercial web only; $c=2$: E-Commerce and non-commercial web; $c=3$: E-government, e-commerce, and the non-commercial web.

While those have quite different characteristics as a platform, all of them represent important movements within the FIM market for the Web (Maler & Reed, 2008; Hühnlein *et al*, 2010). This analysis will allow us to illustrate the field of FIM for the Web, further validate our empirical findings, linking the systems to our identified market segments, and qualitatively discuss some relevant deployment characteristics resulting from the differences between the platforms.

CardSpace

Microsoft has presented CardSpace (Cameron & Jones, 2007) as a more advanced follow-up to Passport with superior privacy-related features (Kormann & Rubin, 2000). Although criticisms of CardSpace do exist (Gajek *et al*, 2009), it is considered much more secure and privacy-friendly than, for example, Passport or OpenID (Maler & Reed, 2008), as it is founded on the rules of identity (Cameron & Jones, 2007), which are held in high regard by the IT security research community. However, in terms of market success, CardSpace has been outperformed by other solutions, even though a copy of it has shipped with every copy of Windows from Vista onwards. In the past, Microsoft has been able to leverage the market influence of Windows to make other related systems such as Internet Explorer successful. Our empirical results indicate that security and privacy are minor factors, and thus we conclude that the failure of Passport cannot be related to its dearth of appropriate privacy and security options. This conclusion is consistent with the success that Passport is now having in the market under its new product name, Windows Live ID. Therefore, the lack of trust that many researchers have theorized to be the cause of Passport's failure may be directed toward the provider Microsoft rather than toward the technology itself (Hühnlein *et al*, 2010). Recently, CardSpace has started implementing anonymous credentials on top of its existing user-controlled design. Thus, it appeals mainly to pioneers, a consumer segment with a low WTP, and also has some limited appeal to average users. However, it seems unclear whether the difference in WTP between anonymous credentials and user control can cover the higher transaction costs. For the entire sample, the switch from user-centric to anonymous credentials can be interpreted as going from the design option with the third highest WTP to the option with the second highest WTP. However, the attributes of Passport/Live ID already matched the option with the highest WTP associated with it.

OpenID

OpenID (Recordon & Reed, 2006) was originally developed for use in the LiveJournal online community as a lightweight, decentralized way to authenticate users making comments (Maler & Reed, 2008). It utilizes user-supplied web addresses to identify services providing identity information and thus supports free choice and even self-hosting for such services. Although there have been several security problems with OpenID (Sovis *et al*, 2010), OpenID has still seen rather broad adoption. It is supported by more than 50,000 web services offering authentication via OpenID, and there are hundreds of millions of OpenID-enabled user accounts with identity-providing services including Google, Twitter, and Yahoo! This indicates that the level of identity certification offered (which is out of scope for OpenID and most of its identity providers) is not one of the major factors influencing the success of FIM systems. Furthermore, possible privacy breaches have not been a major challenge for OpenID. Finally, OpenID does not offer many features that are deemed necessary for use in business to consumer e-commerce; it is targeted mainly at Web 2.0 sites with user-generated content. All of these observations are in line with our empirical results. OpenID seems to have very successfully addressed the needs of the low-value segments of the identity management market and to have also gained some traction in interoperability-centric segments due to its increased usage by service providers. As OpenID offers identity intermediation and a broad applicability, its success aligns with our empirical findings. It is a representative of the product category with the highest WTP across our entire sample. It is also in the preferred product category for followers. For the consumer segment of average users, it represents the category with the second highest WTP, topped only by anonymous credentials. However, the difference in WTP here is only €0.43, which is unlikely to refinance the associated infrastructural investments. Anonymous credentials require a PKI with redundant certification authorities (Camenisch & Van Herreweghen, 2002), and even less costly PKI deployments

allowing only for certification cannot be operated on such margins (Roßnagel, 2006). If OpenID was marketed with the option of legally binding authentication, it would also be in the preferred product category for the consumer segment of Risk Averse, which has the highest overall WTP associated with it, and is not addressed by other products currently in the market. As the OpenID standard considers authentication out of scope, arbitrary levels of identity certification can be realized. Thus, a certifying German identity provider for OpenID and similar protocols should be very viable.

Facebook

The online community site Facebook has recently implemented a single sign-on solution that is specific to the platform and that transmits additional information (such as the user's social graph) along with traditional identity information. The core FIM functionality is part of Facebook's 'Login Button' and 'Registration' plugins, but those are bundled with additional 'Social Plugins', that is, the 'Like Button' and 'Graph API' as part of the 'Facebook for Websites' product (Facebook for web developers, 2012).

The system has gained even greater traction than OpenID, as is illustrated by overall user interest (Hühnlein *et al*, 2010), reports from individual identity-providing services (CrowdVine, 2009), as well as statistics estimating number of relying parties and usage (Landau and Moore, 2011). Again, this illustrates the explosive growth experienced by some identity management solutions. Once again, privacy concerns, while broadly discussed, do not seem to substantially impact the adoption process, which is consistent with our empirical results, indicating that many users are happy to have their information hosted under the control of a service provider. One possible explanation could be based on the results of Dinev *et al* (2013), who have shown that perceived benefits of information disclosure negatively influence perceived risk, which in turn negatively influences perceived privacy. In terms of interoperability, Facebook has managed to expand its FIM from a platform-internal support for browser games and other profile plug-ins to a full-fledged FIM system serving as a basis for additional services (such as the Facebook 'like' buttons). Facebook probably offers the widest range of applications in this analysis of contemporary FIM systems, and thus the most flexible applicability. The service is offered for free but is used to build user profiles for advertising. Our empirical results indicate (correctly) that such an identity intermediation service could appeal to a sizable segment of the market. The degree to which Facebook can certify user information is debatable, but it can back its user information up with a wide range of user profiles, and has offered advertisers access to customers' full profiles in the past, which amounts to a similar functionality. Thus, Facebook has an appeal that is quite similar to that of OpenID, that is, it should also appeal to followers, average users, and ultimately the whole sample, which is well in line with our observations on the macro level. As Facebook offers several additional (potentially useful) services, it should be no surprise that overall Facebook's FIM mechanism has achieved a tremendous success in the market.

Discussion

As we observed in the previous section, lightweight systems that only support user-generated claims are currently dominating systems that offer more elaborate security and privacy features. The hypergrowth (Shapiro & Varian, 1999) that has been observed for OpenID and other recent identity management initiatives may be seen as evidence of network effects in the context of web identity management (Hühnlein *et al*, 2010). It is especially remarkable that OpenID has managed to gain a significant number of users as a result of a Web 2.0 grassroots effort, whereas systems like CardSpace have failed to reach a critical mass. This may demonstrate a strong demand for single sign-on in that (fractured) domain. However, the characteristics of the services provided are a question that our empirical results do not address, and further research must be conducted in this field. Furthermore, the market success of Facebook's identity management solution, in spite of the privacy problems associated with Facebook (which has been labeled a 'privacy train wreck', Boyd, 2008) seem to demonstrate that systems that even make more personal information (i.e., the user's social graph) available to third parties can have a considerably higher adoption rate: First, even though experts and some part of the population are dissatisfied with Facebook's privacy, it is still very heavily used as a social network. Second, even though the introduction of Facebook's identity services introduced additional privacy problems, it is still the most successful one in terms of user interest (Hühnlein *et al*, 2010) and in terms of relying parties and usage (Landau and Moore, 2011). One possible explanation based on the model of Dinev *et al* (2013) could be that the perceived benefits of disclosing private information on Facebook reduce the perceived risk and as a consequence have a positive influence on perceived privacy. Both of these findings contradict some of the existing conventional assumptions (Zibuschka & Roßnagel, 2012) regarding success factors for FIM systems in the literature. Technological solutions seem to have a limited influence on user trust; instead, prospective users tend to trust the institutions behind the technologies (McKnight *et al*, 2002). Our findings demonstrate that users do not exhibit a considerable WTP for control over their data, even before considering network effects. The minor role of privacy and security should also affect the adoption of anonymous credentials-based systems. For users to gain meaningful reduced sign-on capabilities across the web, the system that they use must be widely adopted, and the underlying protocol must be implemented by a wide range of service providers (Zibuschka & Roßnagel, 2008). Thus, we assume that utility for all participants in the FIM platform partially depends on adoption by other stakeholders, indicating indirect

network effects (Katz & Shapiro, 1994) with positive feedback: if more users adopt a single sign-on system, more services will adopt it and vice versa. This suggests that identity management systems should be designed to target sizable user segments. The findings of this study may guide such an endeavor, both indicating which user preferences may be most relevant and demonstrating what properties a system targeting a broad group of users should have.

Conclusion

FIM has emerged as a promising technology for user authentication and for distributing identity information across different domains. With the promise of a single sign-on for different domains, FIM can help users to surf the web more conveniently. In principle, there seems to be a market for FIM because all segments have substantial WTP ranging from €3 to €48 per year. The differences are mainly driven by psychographics and demographics. As the pioneers in this markets seem to have a rather low WTP, penetration pricing seems to be a beneficial strategy for FIM providers. The price can be increased when the followers are willing to adopt the innovation as well. This aligns with the fact that systems in the market today are often offered for free, unless providing, for example, advanced levels of certification. We also find that users who exhibit a high level of trust in general and are willing to take risks seem to be more or less out of the market given their low WTP; such respondents in our study were excluded in the cluster analysis because they were not willing to spend any money on any identity management system.

Our results indicate that privacy concerns are of little importance. Although design-oriented research in this domain, especially in engineering and computer science, assumes a need for more secure systems and systems that guarantee a higher level of privacy, our results indicate that prospective users do not value such features as extensively as envisioned by their designers. The results of our conjoint analysis provide evidence that consumers prefer systems in which an intermediary takes responsibility for the user data being provided. This micro-level finding is also reflected in the macro-level data. Simple sign-on systems with questionable privacy levels, like the solutions provided by Facebook, experience very impressive adoption rates and apparently gain stronger traction than more secure and privacy-friendly solutions. If users benefit from systems (for example, because they provide a higher level of convenience), they are willing to refrain from demanding high privacy levels and are even willing to share their data. As privacy-enhancing identity management systems are generally believed to be critical for protecting users' online privacy (Hansen *et al*, 2004), these results suggest that online privacy technologies play a minor role in general, as users do not seem willing to pay for a critical building block of that infrastructure.

However, those results only apply to the case of FIM for the Web in the sense of Maler & Reed (2008) and Hühnlein *et al* (2010), and only for Germany. Related markets such as government eID solutions in other cultural backgrounds are not covered by our results, even though the analyses presented in this contribution show that our empirical findings for Germany align with the global market of FIM for the Web. A recent study (Lancelot Miltgen & Peyrat-Guillard, forthcoming) has revealed how privacy and control perception varies across European countries. For example, their results show that people in southern European countries are more likely to trust and disclose information than people from eastern European countries who are more reluctant.

Furthermore, as we needed to retain a valid instrument for our survey, we had to restrict the number of factors under investigation. We performed a pre-study to identify the most relevant factors; however, additional factors such as liability or accountability may also play a significant role, especially in other cultures and markets.

The basic assumption of our work is that users pay for the service. The reasons for this basic assumption are that we (1) want to measure user preferences for system characteristics (security, privacy, application area) based on WTP and (2) focus on the prevalent pricing model as FIM providers going beyond the basic configuration (1-1-1), such as PKI or eID initiatives, usually charge fees for their services (Roßnagel & Lippmann, 2005). Similar infrastructures would be required for configurations offering the highest level of privacy (x-3-x) (Camenisch & van Herreweghen, 2002), and would certainly incur significant costs, going even beyond PKI for the current technologies. Those levels are not covered by the FIM systems currently offered for the web; however, there have been several initiatives to push such systems for web-based scenarios. This assumption is a limitation in terms of the likely business model for such identity services, as there might be good reasons to offer FIM systems to users free of charge. For example, online service providers such as Facebook and Google might offer free and privacy-friendly credentials that help to ensure that their customers remain 'logged in' to their services when performing secure identity-based transactions. Further, new players, who enter the identity provider marketplace, might offer free identity credentials to their customers in order to attract a high number of new customers. This also offers an interesting avenue for future research that could focus on customers that show no WTP for such systems (139 respondents in our sample). There might also be alternative revenue schemes, for example, website operators pay the FIM provider. This alternative revenue schemes are, however, out of scope of this paper and might provide further interesting avenues for future research. We note that this strategy did not work very well for Passport, and the technologically fully compatible but significantly more successful (Hühnlein *et al*, 2010; Landau & Moore, 2011) Passport follow-up Windows Live ID (Cameron, 2006) does not charge relying parties any longer.

Furthermore, as we surveyed system properties that would benefit the users, such as privacy and broad applicability, it is unclear why service providers should have a WTP if users do not prefer systems exhibiting those characteristics.

Further, we focused on users' overall WTP for FIM systems for the Web per year. We did not examine how this WTP would be distributed between different entities in identity meta-systems such as the ones described in Cameron & Jones (2007) and Schwartz (2011). This would be another interesting avenue for further research.

We hypothesize that indirect network effects in this multi-sided market are a main driver of adoption. Providers of FIM should therefore focus more on the chicken-and-egg-problem (Evans, 2003) and develop relevant strategies (such as fostering sub-network adoption or piggybacking) (Ozment & Schechter, 2006), as embodied by Facebook's bundling of FIM-related products.

It seems prudent to focus on creating value for the user rather than implementing the most sophisticated security and privacy features, especially as such features are not valued as highly in services that users perceive as useful (Dinev *et al*, 2013).

About the authors

Heiko Roßnagel is Head of the Competence Team Identity Management at the Fraunhofer-Institute for Industrial Engineering. His research interests are in the areas of security, privacy, and identity management with a focus on technology development and adoption.

Jan Zibuschka is Senior Scientist at the Fraunhofer-Institute for Industrial Engineering. He published in several areas of economics of security, including the design of market-compliant solutions for privacy in location-based services and cost-efficient approaches for web identity management and single sign-on.

Oliver Hinz is Professor of Electronic Markets at the TU Darmstadt. His research has been published or is forthcoming in journals like *Information System Research* (*ISR*), *Management Information Systems Quarterly* (*MISQ*), *Journal of Marketing*, *Journal of Management Information Systems* (*JMIS*), *Decision Support Systems* (*DSS*), *Journal of Business Research* (*JBR*), and in a number of proceedings (e.g., *ICIS*, *ECIS*, *PACIS*).

Jan Muntermann is Professor of Electronic Finance and Digital Markets at Georg-August University Göttingen. His research interests include decision support systems, design science, and IT Governance, especially in the fields of E-Finance and Electronic Markets. His research appeared in *Decision Support Systems* (*DSS*), *European Journal of Information Systems* (*EJIS*), and *ICIS* proceedings.

References

ACQUISTI A (2008) Identity management, privacy and price discrimination. *IEEE Security & Privacy* **6(2)**, 46–50.

ARD; ZDF. (2010) ARD – ZDF – onlinestudie: Internetnutzer in Prozent. [WWW document] http://www.ard-zdf-onlinestudie.de/index.php?id=onlinenutzungprozen (accessed 20 December 2010).

AUTY S (1995) Using conjoint analysis in industrial marketing: the role of judgement. *Industrial Marketing Management* **24(3)**, 191–206.

BACKHOUSE J, HSU C and MCDONNELL A (2003) Toward public-key infrastructure interoperability: lessons from an information security standard accreditation scheme. *Communications of the ACM* **46(6)**, 98–100.

BAKOS Y (1991) Information links and electronic marketplaces: the role of interorganizational information systems in vertical markets. *Journal of Management Information Systems* **8(2)**, 31–52.

BARKER RM, DOS SANTOS BL, HOLSAPPLE CW, WAGNER WP and WRIGHT AL (2007) Tools for building information systems. In *Handbook of Industrial Engineering: Technology and Operations Management, Third Edition* (SALVENDY G, Ed), pp 65–109, John Wiley & Sons, Inc, Hoboken, NJ.

BERENDT B, GÜNTHER O and SPIEKERMANN S (2005) Privacy in e-commerce: stated preferences *vs*. actual behavior. *Communications of the ACM* **48(4)**, 101–106.

BHATTI R, BERTINO E and GHAFOOR A (2007) An integrated approach to federated identity and privilege management in open systems. *Communications of the ACM* **50(2)**, 81–87.

BITKOM. (2011) Datenschutz im Internet. Whitepaper, BITKOM, Berlin. Available from [WWW document] http://www.bitkom.org/files/documents/BITKOM_Publikation_Datenschutz_im_Internet.pdf.

BOYD D (2008) Facebook's privacy trainwreck: exposure, invasion, and social convergence. *Convergence: The International Journal of Research into New Media Technologies* **14(1)**, 13–20.

BRAZELL JD, DIENER CG, KARNIOUCHINA E, MOORE WL, SÉVERIN V and ULDRY P (2006) The no-choice option and dual response choice designs. *Marketing Letters* **17(4)**, 255–268.

BURGESS L (2007) Discrete Choice Experiments (Computer Software), Department of Mathematical Sciences, University of Technology, Sydney. Available from [WWW document] http://crsu.science.uts.edu.au/choice/.

CAMENISCH J and VAN HERREWEGHEN E (2002) Design and implementation of the idemix anonymous credential system. In *Proceedings of the 9th ACM Conference on Computer and Communications Security (ACM CCS'02)* (ATLURI V, Ed), pp 21–30, ACM, Washington, D.C.

CAMERON K (2006) Windows live ID whitepaper. [WWW document] http://www.identityblog.com/?p=509 (accessed 19 September 2013).

CAMERON K and JONES MB (2007) Design rationale behind the identity metasystem architecture. In *ISSE/SECURE 2007 Securing Electronic Business Processes*. (POHLMANN N, REIMER H and SCHNEIDER W, Eds), pp 117–129, Vieweg+Teubner, Wiesbaden.

CHAPMAN CN, LOVE E and ALFORD JL (2008) Quantitative early-phase user research methods: hard data for initial product design. In *Proceedings of the 41st Hawaii International Conference on System Sciences. 37. IEEE* (SPRAGUE RH, Ed) IEEE, Waikoloa, HI.

CHILDERS TL (1986) Assessment of the psychometric properties of an opinion leadership scale. *Journal of Marketing Research* **23(2)**, 184–188.

CLONINGER CR (1994) *The Temperament and Character Inventory (TCI): A Guide to its Development and Use*. Center for Psychobiology of Personality, Washington University, St. Louis, MO.

COSTA PT and MCCRAE RR (1992) *Revised NEO Personality Inventory (NEO-PI-R) and NEO Five-Factor Inventory (NEO-FFI) Professional Manual*. Psychological Assessment Resources, Odessa, FL.

CrowdVine. (2009) OpenID: CrowdVine blog [WWW document] http://blog.crowdvine.com/tag/openid/ (accessed 16 october 2009).

CUMMINGS R and TAYLOR L (1999) Unbiased value estimates for environmental goods: a cheap talk design for the contingent valuation method. *American Economic Review* **89**(**3**), 649–665.

DAY J and VENKATARAMANAN M (2006) Profitability in product line pricing and composition with manufacturing commonalities. *European Journal of Operations Research* **175**(**3**), 1782–1797.

DE CLERQ J (2002) Single sign-on architectures. In *Infrastructure Security*. (DAVIDA G, FRANKEL Y and REES O, Eds), pp 40–58, Springer, Berlin, Heidelberg.

DHAMIJA R and DUSSEAULT L (2008) The seven flaws of identity management: usability and security challenges. *IEEE Security & Privacy* **6**(**2**), 24–29.

DINEV T, XU H, SMITH JH and HART P (2013) Information privacy and correlates: an empirical attempt to bridge and distinguish privacy-related concepts. *European Journal of Information Systems* **22**(**3**), 295–316.

European Commission. (2011) SPECIAL EUROBAROMETER 359 – Attitudes on Data Protection and Electronic Identity in the European Union. Wave 74.3. TNS Opinion & Social [WWW document] http://ec.europa.eu/public_opinion/archives/ebs/ebs_359_en.pdf (accessed 19 September 2013).

EVANS D (2003) Some empirical aspects of multi-sided platform industries. *Review of Network Economics* **2**(**3**), 191–209.

Facebook for web developers. (2012) Facebook for websites. [WWW document] https://developers.facebook.com/docs/web/ (accessed 19 September 2013).

FU K, SIT E, SMITH K and FEAMSTER N (2001) Dos and don'ts of client authentication on the web. In *Proceedings of the 10th Conference on USENIX Security Symposium* (WALLACH DL, Ed), USENIX Association, Washington DC.

GAJEK S, SCHWENK J, STEINER M and XUAN C (2009) Risks of the cardspace protocol. In *Information Security* (SAMARATI P, YUNG M, MARTINELLI F and ARDAGNA C, Eds), pp 278–293, Springer, Berlin, Heidelberg.

GELMAN A, CARLIN JB and HAL SS (2004) *Bayesian Data Analysis*. Chapman & Hall/CRC, Boca Raton.

GENSLER S, HINZ O, SKIERA B and THEYSOHN S (2012) Willingness-to-pay estimation with choice-based conjoint analysis: addressing extreme response behavior with individually adapted designs. *European Journal of Operational Research* **219**(**2**), 368–378.

GREEN PE and KRIEGER AM (1991) Segmenting markets with conjoint analysis. *The Journal of Marketing* **55**(**4**), 20–31.

GREENWALD S, OLTHOFF K, RASKIN V and RUCH W (2004) The user non-acceptance paradigm: INFOSEC's dirty little secret. In *Proceedings of the 2004 Workshop on New Security Paradigms* (HEMPELMANN C and RASKIN V, Eds), pp 35–43, ACM, Nova Scotia.

HAEUSEL HG (2000) *Der Umgang mit Geld und Gut in seiner Beziehung zum Alter, Dissertation*. Technical University of Munich, Munich, Germany.

HANSEN M, BERLICH P, CAMENISCH J, CLAUß S, PFITZMANN A and WAIDNER M (2004) Privacy enhancing identity management. *Information Security Technical Report* **9**(**1**), 35–44.

HINZ O, HANN IH and SPANN M (2011) Price discrimination in e-commerce? An examination of dynamic pricing in name-your-own-price markets. *Management Information Systems Quarterly* **35**(**1**), 81–98.

HORNUNG G and SCHNABEL C (2009) Data protection in Germany I: the population census decision and the right to informational self-determination. *Computer Law & Security Review* **25**(**1**), 84–88.

HÜHNLEIN D, ROßNAGEL H and ZIBUSCHKA J (2010) Diffusion of federated identity management. In *Sicherheit 2010* (FREILING FC, Ed), pp 25–36, Köllen Druck+Verlag, Bonn.

IVES B, WALSH KR and SCHNEIDER H (2004) The domino effect of password reuse. *Communications of the ACM* **47**(**4**), 75–78.

JACKSON DN (1994) *Jackson Personality Inventory: Revised Manual*. Research Psychologists Press, Port Huron.

JØSANG A, ZOMAI M and SURIADI S (2007) Usability and Privacy in Identity Management Architectures. In *Proceedings of the fifth Australasian Symposium on ACSW Frontiers* (BRANKOVIC L, CODDINGTON PD, RODDICK JF, STEKETEE C, WARREN JR and WENDELBORN AL, Eds), Australian Computer Society, Ballarat.

KARNIOUCHINA E, MOORE WL, VAN DER RHEE B and VERMA R (2009) Issues in the use of ratings-based versus choice-based conjoint analysis in operations management research. *European Journal of Operations Research* **197**(**1**), 340–348.

KATZ ML and SHAPIRO C (1994) Systems competition and network effects. *Journal of Economic Perspectives* **8**(**2**), 93–115.

KOHLI R and KRISHNAMURTI R (1989) Optimal product design using conjoint analysis: computational complexity and algorithms. *European Journal of Operations Research* **40**(**2**), 186–195.

KORMANN D and RUBIN A (2000) Risks of the passport single signon protocol. *Computer Networks* **33**(**1–6**), 51–58.

KRIEGER AM and GREEN PE (1996) Modifying cluster-based segments to enhance agreement with an exogenous response variable. *Journal of Marketing Research* **33**(**3**), 351–363.

KROLO J, SILIC M and SRBLJIC S (2009) Security of web level user identity management. In *MIPRO 2009 – Proceedings of the Information Systems Security* (ČIŠIĆ D, HUTINSKI Ž, BARANOVIĆ M, MAUHER M and DRAGŠIĆ V, Eds), Croatian Society for Information and Communication Technology, Electronics and Microelectronics, Opatija.

LANCELOT MILTGEN C and PEYRAT-GUILLARD D (forthcoming) Cultural and generational influences on privacy concerns: a qualitative study in seven European countries. *European Journal of Information Systems*. advance online publication, 30 July 2013; doi:10.1057/ejis.2013.17.

LANDAU S and MOORE T (2011) Economic tussles in federated identity management. In *The Tenth Workshop on Economics of Information Security (WEIS 2011)* (MOORE T and FRIEDMAN A, Eds), George Mason University, Fairfax, VA.

LICHTENSTEIN DR, RIDGWAY NM and NETEMEYER RG (1993) Price perceptions and consumer shopping behavior: a field study. *Journal of Marketing Research* **30**(**2**), 234–245.

LIEBERMANN Y and STASHEVSKY S (2002) Perceived risks as barriers to internet and e-commerce usage. *Qualitative Market Research* **5**(**4**), 291–300.

LOPEZ J, OPPLIGER R and PERNUL G (2004) Authentication and authorization infrastructures (AAIs): a comparative survey. *Computers & Security* **23**(**7**), 578–590.

MALER E and REED D (2008) The venn of identity: options and issues in federated identity management. *IEEE Security & Privacy* **6**(**2**), 16–23.

MANNAN M and VAN OORSCHOT PC (2007) Using a personal device to strengthen password authentication from an untrusted computer. In *Proceedings of the 11th international Conference on Financial Cryptography and 1st international Conference on Usable Security* (DIETRICH S and DHAMIJA R, Eds), pp 88–103, Springer, Scarborough, Trinidad and Tobago.

MCKNIGHT DH, CHOUDHURY V and KACMAR C (2002) Developing and validating trust measures for e-commerce: an integrative typology. *Information Systems Research* **13**(**3**), 334–359.

MILLER K, HOFSTETTER R, KROHMER H and ZHANG J (2011) How should we measure consumers' willingness to pay? An empirical comparison of state-of-the-art approaches. *Journal of Marketing Research* **48**(**1**), 172–184.

MOORTHY S, RATCHFORD B and TALUKDAR D (1997) Consumer information search revisited: theory and empirical analysis. *Journal of Consumer Research* **23**(**4**), 263–277.

MUELLER ML, PARK Y, LEE J and KIM T (2006) Digital identity: how users value the attributes of online identifiers. *Information Economics and Policy* **18**(**4**), 405–422.

NATTER M and FEURSTEIN M (2002) Real world performance of choice-based conjoint models. *European Journal of Operations Research* **137**(**2**), 448–458.

NEUMANN PG (1994) Risks of passwords. *Communications of the ACM* **37**(**4**), 126.

OZMENT A and SCHECHTER SE (2006) Bootstrapping the adoption of internet security protocols. In *Proceedings of the Fifth Workshop on the Economics of Information Security (WEIS 06)* (ANDERSON R, Ed), University of Cambridge, Cambridge.

PUNJ G and STEWART DW (1983) Cluster analysis in marketing research: review and suggestions for application. *Journal of Marketing Research* **20**(**2**), 134–148.

RECORDON D and REED D (2006) OpenID 2.0: a platform for user-centric identity management. In *Proceedings of the second ACM Workshop on Digital Identity Management* (JUELS A, Ed), pp 11–16, ACM Press, Alexandria, VA.

ROßNAGEL H and LIPPMANN S. (2005) Geschäftsmodelle für signaturgesetzkonforme trust center. In *Wirtschaftsinformatik 2005* (ECKERT S, FERSTL OK, ISSELHORST T and SINZ E, Eds), pp 1167–1186, Physica Verlag, Heidelberg.

ROßNAGEL H (2006) On diffusion and confusion – why electronic signatures have failed. In *Trust and Privacy in Digital Business* (FISCHER-HÜBNER S, FURNELL S and LAMBRINOUKDAKIS C, Eds), pp 71–80, Springer, Berlin, Heidelberg.

SCHLÄGER C, SOJER M, MUSCHALL B and PERNUL G (2006) Attribute-based authentication and authorisation infrastructures for e-commerce providers. In *E-Commerce and Web Technologies* (BAUKNECHT K, PRÖLL B and WERTHNER H, Eds), pp 132–141, Springer, Berlin, Heidelberg.

SCHWARTZ A (2011) Identity management and privacy: a rare opportunity to get it right. *Communications of the ACM* **54(8)**, 22–24.

SHAPIRO C and VARIAN HR (1999) *Information Rules: A Strategic Guide to the Network Economy*. Harvard Business School Press, Boston, MA.

SHOSTACK A and SYVERSON P (2004) What price privacy? (And why identity theft is about neither identity nor theft). In *Economics of Information Security* (CAMP LJ and LEWIS S, Eds), pp 129–142, Springer, Berlin, Heidelberg.

SOVIS P, KOHLAR F and SCHWENK J (2010) Security analysis of OpenID. In *Sicherheit 2010 Proceedings* (FREILING FC, Ed), pp 329–340, Köllen Druck+ Verlag, Bonn.

STREET DJ and BURGESS L (2007) *The Construction of Optimal Stated Choice Experiments: Theory and Methods*. Wiley-Interscience, New Jersey.

TSANG PP, AU MH, KAPADIA A and SMITH SW (2007) Blacklistable anonymous credentials: blocking misbehaving users without TTPs. In *Proceedings of the 14th ACM conference on Computer and Communications Security* (NING P, Ed), pp 72–81, ACM Press, Alexandria, VA.

WARD JH (1963) Hierarchical grouping to optimize an objective function. *Journal of the American Statistical Association* **58(301)**, 236–244.

WHITLEY EA (2012) On technology neutral policies for e-identity: a critical reflection based on U.K. identity policy. *Journal of International Commercial Law and Technology* **8(2)**, 134–147.

WHITLEY EA and HOSEIN IR (2008) Doing the politics of technological decision making: due process and the debate about identity cards in the U.K. *European Journal of Information Systems* **17(6)**, 668–677.

WOHLGEMUTH S and MÜLLER G (2006) Privacy with delegation of rights by identity management. In *Emerging Trends in Information and Communication Security* (MÜLLER G, Ed), pp 175–190, Springer, Berlin, Heidelberg.

WU J and AYALAGAYTAN EA (2013) The role of online seller reviews and product price on buyers' willingness-to-pay: a risk perspective. *European Journal of Information Systems* **22(4)**, 416–433.

ZIBUSCHKA J and ROßNAGEL H (2008) Implementing strong authentication infrastructure interoperability with legacy systems. In *Policies and Research in Identity Management* (DE LEEUW E, FISCHER-HÜBNER S, TSENG J and BORKING J, Eds), pp 149–160, Springer, Boston.

ZIBUSCHKA J and ROßNAGEL H (2012) On some conjectures in it-security: the case for viable security solutions. In *Sicherheit 2012 Proceedings* (SURI N and WAIDNER M, Eds), pp 25–33, Köllen Druck+Verlag, Bonn.

Supplementary information accompanies this article on the *European Journal of Information Systems* website (www.palgrave-journals.com/ejis)