Understanding the Determinants of Privacy-ABC Technologies Adoption by Service Providers

Ahmad Sabouri

Understanding the Determinants of Privacy-ABC Technologies Adoption by Service Providers

Ahmad Sabouri

Deutsche Telekom Chair of Mobile Business & Multilateral Security,
Goethe University Frankfurt,
Theodor-W.-Adorno-Platz 4, 60323 Frankfurt, Germany
ahmad.sabouri@m-chair.de

Abstract. As using online services penetrates deeper in our everyday life, lots of trust-sensitive transactions are carried out electronically. In this regard, a big challenge is to deal with proper user authentication and access control without threatening the users' privacy. However, commonly used strong authentication schemes fail to address important privacy requirements. In this paper, we focus on an emerging type of digital certificates, known as Privacy-preserving Attribute-based Credentials (Privacy-ABCs), which allow privacy and security go hand-in-hand. So far, there has been no systematic study on the potential factors that have influence on the adoption of Privacy-ABCs by service providers. Thus, we developed a conceptual model of the relevant factors based on well-established theories and our practical experience with trialing Privacy-ABCs, and evaluated the model through expert surveys.

Keywords: Privacy-preserving Attribute-based Credentials, Anonymous Credentials, Technology Adoption, Expert Surveys.

1 Introduction

Nowadays, usernames and passwords are the most commonly used authentication schemes. However, the hassle of managing different usernames and passwords grows as the number of electronic services increases. This, on the one hand, raises security risks because many users tend to reuse the same password for different services. On the other hand, it introduces privacy threats for cross-linking activities of the users in different domains as it is highly probable to be able to correlate different identifiers of the same person [36] because they typically prefer to choose the same or similar usernames for their various accounts.

An alternative solution to improve the security problem is to employ strong authentication techniques such as digital certificates. Nonetheless, the most commonly used strong authentication techniques do not follow the Privacy-by-Design [6] principle of *Data Minimization*. For instance, the use of X509 certificates causes "Over-Identification", as it mandates the users to reveal all the attested

attributes in the certificate so that the validity of the digital signature is preserved, even if only a subset of attributes is required for the authentication purpose. Using online federated authentication and authorization techniques such as OpenID, SAML, Facebook Connect, and OAuth could support the minimal disclosure principal and allow the users to provide the service providers with only the requested information rather than the whole user's profile stored at the Identity Service Provider (IdSP). However, all these protocols suffer from a so-called "Calling Home" problem, meaning that for every authentication transaction the user is required to contact the IdSP (e.g., Facebook, Gmail, OpenID Provider). This introduces privacy risks to both users and service providers.

The focus of this paper is on a promising type of digital certificates called Privacy-preserving Attribute-based Credentials (Privacy-ABCs) that provide a strong basis for secure yet privacy-enhanced access control systems. Privacy-ABCs offer a solution to cope with *Minimal Disclosure* of attributes as well as supporting *Partial Identities*. Privacy-ABC users can obtain credentials from their IdSPs and when authenticating to different service providers, they can produce *unlinkable Privacy-ABC tokens* containing only the required subset of information available in the credentials without involving the IdSP or any third party in the process. Therefore, they can help overcome the "Over-Identification" and "Calling Home" problems. The prominent instantiations of such Privacy-ABC technologies are Microsoft U-Prove[1] and IBM Idemix[2]. Both of these technologies are studied in depth by the EU-funded project ABC4Trust, where a common architecture for Privacy-ABCs was designed, implemented and verified in two real-life trials [28].

Privacy-ABCs are emerging technologies that are not yet properly adopted. There have been a handful of proposals on how to realize a Privacy-ABC system in the literature [4,5]. However, the diversity of their features and implementations hindered their practical use. As Privacy-ABCs are in the pre-adoption phase, our rigorous literature review on drivers and inhibitors of Privacy-ABCs using well-known databases such as JStore, MISQ, AISnet, ACM and IEEE ended up in a limited set. Borking investigated the adoption of Privacy Enhancing Technologies (PETs) in general [3]. Nevertheless, PETs can be very different in their characteristics and their adoption schemes. For instance, Tor[3] is also an example of PETs that can be employed directly by the end users, while in order to have Privacy-ABC technologies operational, at least three entities have to adopt or accept the technology: (1) Credential issuers, which are typically organizations such as governments, banks, and telco operators who have authentic source of data about the users, (2) Service providers, which perform access control to their resources relying on the credential attested by the issuers, (3) Users, who consider using such kind of credentials. Therefore, Privacy-ABCs have special characteristics and effects that make them deserve a separate study. Therefore, this paper focuses on the adoption factors influencing **service providers** and

[1] http://microsoft.com/uprove
[2] http://idemix.wordpress.com/
[3] https://www.torproject.org/

launches the first systematic work based on well-established theories to investigate the (future) adoption of Privacy-ABCs. Understanding the determinants of adoption by service providers is very important in the sense that identifying these factors can facilitate building guidelines for the supporting bodies to pave the road for the further adoption of Privacy-ABCs. Therefore, we developed a conceptual model based on the existing innovation adoption theories and evaluated the factors through expert surveys.

The rest of this paper is organized as follows. In Section 2, we introduce the features and concepts of Privacy-ABCs in more details and also deliver an overview of the theories in the literature explaining innovation adoption. Later, we present our conceptual model of the determinants in Section 3. Then, in Section 4, we present our empirical evaluation of the factors, and later in Section 5 discuss our findings and their implications. In the end, we conclude the paper in Section 6.

2 Theoretical Background

2.1 How Privacy-ABCs Work

A *Credential* is defined to be "a certified container of attributes issued by a credential Issuer to a User" [1]. An *Issuer* vouches for the correctness of the attribute values for a *User* when issuing a credential for her. In an example scenario, Alice as a *User*, contacts the Bundesdruckerei (the German authority responsible for issuing electronic IDs) and after a proper proof of her identity (e.g. showing her old paper-based ID), she receives a digital identity credential containing her first name, surname and birth-date. In the next step, she can seek to access an online Discussion Forum. The service provider provides Alice with the access policy that requires her to deliver an authentic proof of her first name. Using Privacy-ABCs features, Alice has the possibility to derive a minimal authentication token from her identity credential that contains only the first name. As a result, her privacy is preserved by not disclosing unnecessary information (i.e. surname and birth-date). Note that the commonly used digital certificates do not offer such capability as any change in those certificates invalidates the issuers' signature. Another example where Alice could use her Privacy-ABC might be with an online movie rental website, which requires age verification. Alice is able to provide such a proof without actually disclosing her exact birth-date. The proof is done based on complex cryptographic concepts that can show her birth-date attribute in her credential is before a certain date.

2.2 Innovation Adoption

A prominent approach to investigate adoption of new technologies is covered by the Diffusion of Innovation theory (DOI), presented by Rogers [27]. DOI theory sees innovations as being communicated through certain channels over time and within a particular social system. The approach focuses on the way in which

a new technological invention migrates from creation to use. Rogers identified five important attributes of innovations that might influence the decision for their adoption or rejection. The five characteristics of innovations are relative advantage, compatibility, complexity, trialability, and observability, which are valid for both individual and organizational adoption of technology.

Technology-Organization-Environment (TOE) framework was presented by Tornatzky [34] to study the adoption of technological innovations. The framework considers a threefold context for adoption and implementation of technological innovations: technological context, organizational context, and environmental context. The technological context relates to the technologies relevant to the firm such as the current internal practices and equipment, as well as the set of relevant technologies external to the firm. The organizational context describes the characteristics of an organization including firm size, degree of centralization, formalization, complexity of its managerial structure, the quality of its human resources, and the amount of slack resources available internally. Comparing to Rogers' model, TOE includes a new and important component, environmental context. The environment context is the arena in which a firm conducts its business such government and the competitors.

Iacovou et. al. [15] presented a model to investigate the interorganizational systems (IOSs) characteristics that influence firms to adopt IT innovations in the context of Electronic Data Interchange (EDI). In this model, Perceived Benefits is a different factor from the TOE framework, whereas organizational readiness is a combination of the technology and organization context of the TOE framework. Nevertheless, Iacovou et al. included and highlighted external pressure as an important factor.

We have identified the Institutional Theory also to be relevant for our research. Institutional factors including schemas, rules, norms, and routines are crucial in shaping organizational structure and organizational decisions [29]. According to the institutional theory, organizational decisions are not driven purely by rational goals of efficiency, but also by social and cultural factors and concerns for legitimacy. It is posited by DiMaggio and Powell [9] that Coercive isomorphism, known as the pressures from other organizations, Mimetic isomorphism, known as the imitation of structures adopted by others in response to pressures, and Normative isomorphism, known as conformity to normative standards established by external institutions, potentially have influence on the behaviour of an organization.

3 Conceptual Model for Adoption of Privacy-ABCs

Based on the theories explained in the previous section, we constructed a combined conceptual model of the relevant factors that are potentially applicable to Privacy-ABCs adoption. We also propose some factors that are new and specific to the domain of Privacy and characteristics of Privacy-ABCs. The conceptual model presented in Figure 1 incorporates thirteen factors categorized in five groups.

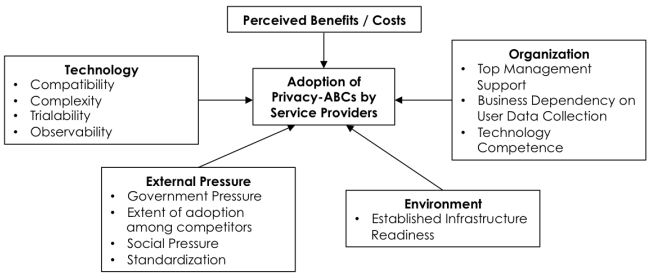

Fig. 1. Conceptual Model for factors influencing adoption of Privacy-ABCs by Service Providers

Technology

Privacy-ABCs are a kind of new technologies for privacy-respecting access control and their characteristics may have a strong influence on the decision of the potential adopters.

Compatibility: refers to the degree to which an innovation is perceived as consistent with the existing values, needs, and past experiences of the potential adopters [27]. Various published studies examined the role of compatibility, and considered it to be an essential determinant of IT innovation adoption [32,24,33,37] and several of them (e.g. [33,37]) found it as a significant driver. Regarding Privacy-ABCs, it is probable that a higher compatibility of their specifications with the existing Identity and Access Management (IAM) protocols and standards that are commonly used increases the likelihood of a positive decision to adopt them, as any change in the IAM processes may affect a wide range of the subsystems.

Complexity: refers the degree to which an innovation is perceived as relatively difficult to understand and use [27]. There have been several works considering the role of complexity in innovation adoption [33,7,16]. Privacy-ABCs are based on difficult cryptographic concepts, which are not easy for people beyond the inventors to understand. On the one hand, following the claim by Borking [3], understanding of Privacy-ABCs for the purpose of adoption requires technical and legal knowledge. On the other hand, Wästlund et. al. [35] claim that the users have difficulties in using these novel technologies. Therefore, we consider Complexity to be a relevant factor in adoption of Privacy-ABCs.

Trialability: refers to the degree to which an innovation may be experimented with and tested on a limited basis [27]. In another word, it concerns how easy it would be for a potential adopter to test (or partially test) the features that the new technology provides. There is always a level of uncertainty for the adopters when they decide to invest on a new innovation and reducing this uncertainty by allowing them to try out the innovation would probably influence their decision. Trialability has been identified to be important in a number studies concerning adoption of a new technology [16,18,25]. Borking [3] also highlights the role of

Trialability for the adoption of PETs in general. Therefore we envision that Privacy-ABCs adoption can be influenced by their Trialability.

Observability: refers to the extent to which the innovations are visible for the outside world [27]. In this regard, Moore and Benbasat [20] consider demonstrability as one type of observability. Unlike many other innovations that have visible results and can be well demonstrated, Privacy-ABCs are very challenging to present. They are not like standalone products and are always integrated into another service in order to perform access control. Therefore, demonstrators have difficulties showing all the added values of Privacy-ABCs in demos.

Perceived Benefits / Costs

It has been indicated in both DOI and Iacovou models that the likelihood of the allocation of the managerial, financial, and technological resources necessary to use that innovation are increased when there is better managerial understanding of the relative advantage of an innovation increases. Employing Privacy-ABCs comes with some direct and indirect costs such as for implementation, education, and change of processes. It can be challenging to find business cases that are enabled by Privacy-ABCs directly, nevertheless, compliance with data protection regulation, less investment in personal data storage and protection, and reduced risk of privacy breaches are the perceptions that can influence Privacy-ABCs adoption.

Organization

Beside the characteristics of an innovation itself, several organizational characteristics of the potential adopters have an influence on their decision to adopt or reject an innovation.

Top Management Support: It has been shown that technology innovation adoption can be influenced by top management support and their attitudes towards change [23,7,33]. The lack of top management support was identified as a key inhibitor in B2B deployment of e-commerce by [31]. Borking [3] also mentioned that top management's attitude towards changes caused by PETs can influence the adoption of PETs. Consequently, it may be the case that top management support increases the likelihood of adoption of Privacy-ABCs.

Business Dependency on User Data Collection: The role of industry sector in which a firm operates has been investigated and identified to have an influence on adoption of IT technologies in [19,26,11]. Indeed, Privacy-ABCs have not been invented only for the use of businesses and enterprises and can be adopted by any other organization. Nevertheless, we experienced in the context of the ABC4Trust EU research project that it is usually more challenging to convince businesses to integrated Privacy-ABCs into their services compared to other organizations such as non-profit ones. That increased the curiosity to have a special look at the case of commercial adopters that might result in a useful impression of the influencing factors. Essentially, the *Business Model* of a company defines

its roadmap. Osterwalder [22] defines the business model to be a conceptual link forming a triangle between strategy, business organization and ICT. Among the elements of a business model, employing Privacy-ABCs can influence the following:

- Product: Adopting Privacy-ABCs allows the customers to reveal less personal information. Therefore, if the business model value proposition is shaped around the users' data (such as Social Networks), the company will be probably more reluctant to employ such kind of technologies. As a result, we expect that dependency of the business to the collected users data plays an important role in the decision for adopting Privacy-ABCs.
- Customer Interface: It is a common practice to conduct targeted marketing and advertisement based on the extra information collected from the users, such as demographic data. Using Privacy-ABCs heavily influence this part as they prevent the service providers from such kind of data collection.

Technology Competence: Technological resources have been consistently identified as an important factor for successful information systems adoption [8,33]. A higher perceived technical competence was also identified by [17] as a key factor in adoption of electronic data interchange. The work by [37] also demonstrated that technology competence significantly drives e-business usage. So, the role of technology competence has been proven in the literature in adoption of many IT innovations. We consider technical competence to be relevant for adoption of Privacy-ABCs as we also experienced in the context of ABC4Trust pilots that typical developers had difficulties to integrate Privacy-ABCs into some services on their own and constant support of technology providers was needed, while developers with scientific background and technical understanding of the technology went through the integration process smoothly. Hence, lack of technical competency can hinder Privacy-ABCs adoption.

External Pressure

As we mentioned earlier, various sources of external pressure may influence the adoption of new innovations. Here we briefly introduce the ones that are relevant for Privacy-ABCs.

Regulatory Pressure: A regulatory body may be the source of coercive pressures [30]. In this regard, there has been movements in the regulatory sectors in Europe introducing more restriction on users' data collection and processing (Art. 6 and 7 of Directive 95/46/EC) as well as secure storage of the collected data (Art. 16 and 17 of Directive 95/46/EC). Consequently, it can be foreseen that organizations will soon feel pressure to start reconsidering their data collection schemes and look for secure solutions that reduces their liability for protecting the users data.

Social Pressure: There have been major incidences recently which we expect them to have an influence on adoption of privacy enhancing technologies in

general. The most well-known incidence was brought up by Edward J. Snowden [4], which indeed highly stimulated the public opinion on the need for a raise of privacy in online environments. So, we expect that social pressure on the service providers will increase and therefore urges them towards employing mechanisms that reduce personal data collection in their processes.

Extent of Adoption among Competitors: The existence of mimetic pressures toward the adoption of innovations by organizations is confirmed in [10] and [13]. Knowing a competitor has adopted an innovation and it has been a success, the firm tends to adopt the same innovation [14]. The work by [30] confirmed the strong role of this factor in adoption of E-Procurement System. It could happen that offering more privacy becomes an advertising parameter especially in countries with more privacy protection culture. Therefore adoption of Privacy-ABCs by the competitors of a firm can motivate the decision makers to follow the same approach not to lose on the trust reputation.

Standardization: It is very typical for industries to employ procedures, processes or protocols that are standardized in order to ensure interoperability and sustainability of their products and services. In this regard, Standardization can become a source of normative isomorphism. There have been standardization projects that are very relevant to Privacy-ABCs and the ABC4Trust architecture [12]. For instance, ISO/IEC 24760 focuses on a framework for identity management and is conducted in 3 parts covering *Terminology and concepts*, *Reference architecture and requirements*, and *Practice*. Such standards have a good potential to influence the future adoption of Privacy-ABCs.

Environment

Here with environment we refer to the external conditions that do not introduce any pressure but can facilitate or hinder adoption of an innovation. For instance, it is more likely to succeed in implementing the idea of a remote movie rental company in a country that has cheaper, faster and more reliable postal services around.

Established Infrastructure Readiness: Electronic IDs have been implemented in various countries around the world, and therefore use of digital certificates for authentication and access control have been leveraged for service providers. Privacy-ABCs have been demonstrated their capabilities to be integrated with the existing eID infrastructure [2]. Furthermore, the European Commission also considered investing on the research for integration of Privacy-ABCs into future electronic IDs [5]. Consequently, having the global infrastructure ready to support Privacy-ABCs, the integration of these technologies into authentication and access control of service providers will be facilitated.

[4] http://en.wikipedia.org/wiki/Edward_Snowden
[5] http://www.futureid.eu/

4 Empirical Evaluation

4.1 Methodology

As Privacy-ABCs are not yet adopted, it is not possible to survey the service providers (adopters/non-adopters) in order to discover the drivers and the inhibitors. Thus, we decided to follow a forecast approach and collect the opinion of the experts from the relevant fields on the importance and influence level of the potential factors we introduced in our conceptual model. We designed a questionnaire containing quantitative and used a 5-point Liker scale from "not important at all" or "not at all influential" to "extremely important" or "extremely influential". Moreover, based on our experience of the ABC4Trust pilots, we made some of the factors more granular and presented them in two questions. That includes the Cost factor, which we presented as *Cost of Integration* and *Cost of Education*, Complexity factor, divided into *Complexity for Developers* and *Complexity for Users*, and the Government Pressure, presented as *Regulations for Data Collection* and *Regulations for Securing the Collected Personal Data*.

We refined the questionnaire in an iterative process performed in four steps with the help of two groups, one *with* dominant knowledge of Privacy-ABCs, and one *without* dominant knowledge of Privacy-ABCs. In the first step, a person with dominant knowledge in the field reviewed the questionnaire to check the technical correctness and readability of the questions. After rounds of discussions a version was ready to be reviewed by the people without dominant knowledge to validate the readability of the questions. After receiving their feedbacks, the questions were modified to improve the readability. In the next step, again a person with dominant knowledge reviewed the changes and the proposed updates. The next version was then distributed to the people without dominant knowledge and as we did not receive further clarification requests, the questionnaire was finalized. In this questionnaire, the respondents were asked to evaluate their level of expertise using the five-level Dreyfus model of skill acquisition. They were also requested to select their domains of expertise from relevant list including "Privacy and Identity Management", "Data Protection", "Policy Maker", and "Software and Services", or specify it if it was not on the list (multiple selection was allowed).

The survey was performed during the ABC4Trust summit event, on 20th of January 2015 in Brussels. The event was one of the best opportunities to get into contact with the experts of the relevant domains as it was broadly advertised via various important channels such as the one from the European Commission. Furthermore, having prestigious guest speakers also increased the chance of attracting stack-holders to the event. During this event, we gave a full day tutorial of Privacy-ABCs to the participants, covering various aspects such as limitation of current Identity Management Systems, how Privacy-ABCs work in theory, their implementation on computers, smartcards and mobile phones, as well as four real-time demos of some scenarios where Privacy-ABCs could improve users' privacy. These demos addressed a wide range of scenarios, namely

Rank	Factor	Mean	St. Dev.
1	Business Model Dependency to Data Collection	3,71	0,22
2	Complexity for Users	3,53	0,39
3	Top Management Support	3,29	0,60
3	Observability	3,29	1,47
5	Trialability	3,24	0,32
6	Cost of Integration	3,19	0,83
7	Regulations for Data Collection	3,12	0,74
7	Complexity for Developers	3,12	0,61
9	Regulations for Securing the Collected Personal Data	2,94	0,68
10	Established Infrastructure Readiness	2,88	0,99
11	Social Pressure	2,71	1,10
12	Compatibility with Existing IdM Infrastructure	2,65	1,49
13	Competition among Service Providers	2,59	0,76
14	Standardization	2,53	0,89
14	Cost of Education	2,53	1,26
16	Technical Competency	2,35	1,12

Table 1. Ranking of the relevant factors for adoption of Privacy-ABCs by service providers based on the experts' opinions

"online university course evaluation system" , "school community interaction platform", "online movie streaming" [6], and "hotel booking" [7]. It is important to note that most of the tutorials and presentations were performed by the partners who were not involved in this study so we avoided unintentional biasing of the audience.

4.2 Results

At the end of the day, the participants were asked to answer the provided questionnaire. From over 80 participants, 20 completed the questionnaire, of which we excluded 3 as the respondents evaluated themselves below "Proficient" (below 4 out of 5). From the remaining respondents (the experts), 10 chose "Privacy and Identity Management", 3 chose "Data Protection", 3 chose "Policy Maker", and 5 chose "Software and Services" as their fields of expertise (multiple selection was allowed).

Table 1 summarizes the influence/importance level of the factors from the experts' perspective along with their ranking. The items ranked from 1 to 7 have a mean value over 3.0, meaning that the experts considered them on average "very" or "extremely" important or influential. The results show that in experts' opinion, "Technical Competency" of the adopters has the least effect on their decision among the others. Nevertheless, all the factors received a mean score over the average (2.0).

[6] https://idemixdemo.mybluemix.net/
[7] https://abc4trust.eu/demo/hotelbooking

5 Implications and Discussion

From a practical point of view, the results give directions to supporting communities showing them where to put their future efforts. To foster adoption of Privacy-ABCs, priority shall be given to the items ranked from 1 to 7 ($mean > 3.0$). In this regard, the opinion of the experts can be reflected in two dimensions:

First, the Privacy-ABCs technology developers shall enrich the implementation of Privacy-ABCs in terms of

- Usability and Risk Communication: Privacy-ABCs such as different anonymity levels or applying predicates over attributes did not exist in the previous generation of access control mechanisms. Thus user interfaces shall be enhanced to appropriately communicate such features. In addition to that, Privacy-ABCs are user-centric approaches and their implementation essentially requires a piece of software to run on behalf of the users. This urges the users to install a client agent to represent them in the protocol steps, which consequently reduces the mobility of the users as they need to have this software on every device they use. In this regard, new deployment schemes reducing the need for client side installation can support reducing the complexity for the users.
- Agile Trial Platforms: Having online services that allow the interested parties to rapidly and with minimal effort integrate Privacy-ABCs for trial purposes can significantly improve their trialability.
- Designing Comprehensive Demos: In our questionnaire we asked the experts to select the most informative demos they saw during the day. The school community interaction platform received the most points (9 votes). The experts mainly mentioned they liked the fact that it was a complete set of scenarios and there were very many roles and a richer set of credentials. This allowed to show similarities and differences in the policies and implementations. However, the university course evaluation demo received the second highest point (6 votes) and the given reason was that the smaller scope made the scenario basic, very clear and easy to understand the benefits.
- Plug-and-Play Libraries: providing robust, rich and plug-and-play libraries along with appropriate documentation can notably facilitate the integration process for the software developers and consequently decrease the integration costs.

The second dimension relates to the dissemination strategies. More effort shall be put to target high-ranked managers and provide them with supporting materials that raise their understanding and awareness of Privacy-ABCs such as what these technologies can offer, how Privacy-ABCs can influence their processes, and what is needed for them to employ Privacy-ABCs. Moreover, the data protection bodies and the policy makers shall try to disseminate the capabilities of Privacy-ABCs to the regulatory authorities so that they become aware of the technical means to enforce minimal data collection regulations.

From a theoretical perspective, our results contribute to the existing theories by delivering a reduced conceptual model (Figure 2) as a result of the expert

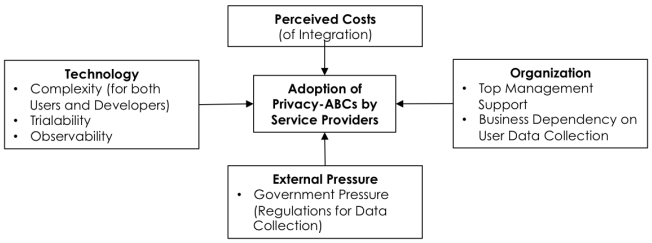

Fig. 2. Reduced Conceptual Model for factors influencing adoption of Privacy-ABCs by Service Providers

surveys. Compared to the literature, our conceptual model introduces a new potential factor for adoption of technologies that limit service providers' access to users' data. The low variance clearly confirms that most of the experts had similar opinion on the role of "Business Model Dependency to Data Collection" and considered it as a key factor for shaping the desire of the service providers to adopt Privacy-ABCs.

The conceptual model also triggers theoretical research to boost the identified factors. More specifically, we see open questions on the methods to efficiently, transparently and explicitly communicate identity and attribute disclosure risks to the users via corresponding user interfaces of Privacy-ABCs.

6 Conclusion

Privacy-ABC technologies are promising mechanisms that allow privacy and security go hand-in-hand. They provide various privacy features such as minimal attribute disclosure as well as unlinkable partial identities. Privacy-ABCs have passed the trial phase and proved their applicability and it is now important to understand how we can push these technologies forward. In this work, we investigated the potential factors that influence adoption of Privacy-ABCs by service provider and empirically evaluated the developed conceptual model through expert surveys. We collected the opinion of the experts during an especial international event where they received a full-day tutorial of various aspects of Privacy-ABCs.

The statistics of the collected opinions show that *Business Model Dependency to Data Collection*, *Complexity for User*, *Top Management Support*, *Observability*, *Trialability*, *Cost of Integration*, *Regulations for Data Collection*, and *Complexity for Developers* are the most important or influential factors impacting the decision of the service providers to employ Privacy-ABCs. These findings put lights on the directions towards which the supporting community should move and imply, despite the common beliefs of recognizing Privacy-ABCs as a redeemer to fight Social Networks, Privacy-ABCs may have higher chance to succeed in their adoption if they first target the service providers in the markets that are not based on users' data.

References

1. A. Sabouri (ed.): Architecture for Attribute-based Credential Technologies - Final Version. Deliverable D2.2, The ABC4Trust EU Project (2014), Available at `https://abc4trust.eu/download/Deliverable_D2.2.pdf`, Last accessed on 2014-11-08
2. Bjones, R., Krontiris, I., Paillier, P., Rannenberg, K.: Integrating anonymous credentials with eids for privacy-respecting online authentication. In: Privacy Technologies and Policy, pp. 111–124. Springer (2014)
3. Borking, J.J.: Why adopting privacy enhancing technologies (pets) takes so much time. In: Computers, Privacy and Data Protection: an Element of Choice, pp. 309–341. Springer (2011)
4. Brands, S.: Untraceable off-line cash in wallet with observers. In: Advances in Cryptology – CRYPTO'93. pp. 302–318. Springer (1994)
5. Camenisch, J., Lysyanskaya, A.: Signature schemes and anonymous credentials from bilinear maps. In: Advances in Cryptology – CRYPTO 2004. pp. 56–72. Springer (2004)
6. Cavoukian, A., et al.: Privacy by design: The 7 foundational principles. Information and Privacy Commissioner of Ontario, Canada (2009)
7. Chong, A.Y.L., Ooi, K.B., Lin, B., Raman, M.: Factors affecting the adoption level of c-commerce: An empirical study. Journal of Computer Information Systems 50(2), 13 (2009)
8. Crook, C.W., Kumar, R.L.: Electronic data interchange: a multi-industry investigation using grounded theory. Information & Management 34(2), 75–89 (1998)
9. DiMaggio, P.J., Powell, W.W.: The Iron Cage Revisited: Institutional Isomorphism and Collective Rationality in Organizational Fields. American Sociological Review 48(2), 147–160 (Apr 1983)
10. Fligstein, N.: The spread of the multidivisional form among large firms, 1919-1979. Advances in Strategic Management 17, 55–78 (1985)
11. Goode, S., Stevens, K.: An analysis of the business characteristics of adopters and non-adopters of world wide web technology. Information technology and Management 1(1-2), 129–154 (2000)
12. Hansen, M., Obersteller, H., Rannenberg, K., Veseli, F.: Establishment and prospects of privacy-abcs. In: Rannenberg, K., Camenisch, J., Sabouri, A. (eds.) Attribute-based Credentials for Trust, pp. 345–360. Springer International Publishing (2015), `http://dx.doi.org/10.1007/978-3-319-14439-9_11`
13. Haunschild, P.R., Miner, A.S.: Modes of interorganizational imitation: The effects of outcome salience and uncertainty. Administrative science quarterly pp. 472–500 (1997)
14. Haveman, H.A.: Follow the leader: Mimetic isomorphism and entry into new markets. Administrative science quarterly pp. 593–627 (1993)
15. Iacovou, C.L., Benbasat, I., Dexter, A.S.: Electronic data interchange and small organizations: adoption and impact of technology. MIS quarterly pp. 465–485 (1995)
16. Kendall, J.D., Tung, L.L., Chua, K.H., Ng, C.H.D., Tan, S.M.: Receptivity of singapore's smes to electronic commerce adoption. The Journal of Strategic Information Systems 10(3), 223–242 (2001)
17. Kuan, K.K., Chau, P.Y.: A perception-based model for edi adoption in small businesses using a technology–organization–environment framework. Information & management 38(8), 507–521 (2001)
18. Martins, C.B., Steil, A.V., Todesco, J.L.: Factors influencing the adoption of the internet as a teaching tool at foreign language schools. Computers & Education 42(4), 353–374 (2004)

19. Miller, N.J., McLeod, H., Young Ob, K.: Managing family businesses in small communities. Journal of Small Business Management 39(1), 73–87 (2001)
20. Moore, G.C., Benbasat, I.: Development of an instrument to measure the perceptions of adopting an information technology innovation. Information systems research 2(3), 192–222 (1991)
21. Moore, G.: Crossing the chasm : marketing and selling disruptive products to mainstream customers. HarperBusiness Essentials, New York, NY (2002)
22. Osterwalder, A., et al.: The business model ontology: A proposition in a design science approach (2004)
23. Premkumar, G., Ramamurthy, K., Crum, M.: Determinants of edi adoption in the transportation industry. European Journal of Information Systems 6(2), 107–121 (1997)
24. Premkumar, G., Roberts, M.: Adoption of new information technologies in rural small businesses. Omega 27(4), 467–484 (1999)
25. Ramdani, B., Kawalek, P.: Sme adoption of enterprise systems in the northwest of england. In: McMaster, T., Wastell, D., Ferneley, E., DeGross, J. (eds.) Organizational Dynamics of Technology-Based Innovation: Diversifying the Research Agenda, IFIP International Federation for Information Processing, vol. 235, pp. 409–429 (2007)
26. Raymond, L.: Determinants of web site implementation in small businesses. Internet Research 11(5), 411–424 (2001)
27. Rogers, E.: Diffusion of innovations. Free Press, New York (2003)
28. Sabouri, A., Krontiris, I., Rannenberg, K.: Attribute-based credentials for trust (abc4trust). In: Trust, Privacy and Security in Digital Business - 9th International Conference, TrustBus 2012, Vienna, Austria, September 3-7, 2012. Proceedings. pp. 218–219 (2012)
29. Scott, W.R.: Institutions and Organizations (Foundations for Organizational Science). SAGE Publications, Inc (2000)
30. Soares-Aguiar, A., Palma-dos Reis, A.: Why do firms adopt e-procurement systems? using logistic regression to empirically test a conceptual model. Engineering Management, IEEE Transactions on 55(1), 120–133 (2008)
31. Teo, T.S., Ranganathan, C., Dhaliwal, J.: Key dimensions of inhibitors for the deployment of web-based business-to-business electronic commerce. Engineering Management, IEEE Transactions on 53(3), 395–411 (2006)
32. Teo, T.S., Tan, M., Buk, W.K.: A contingency model of internet adoption in singapore. International Journal of Electronic Commerce pp. 95–118 (1997)
33. Thong, J.Y.: An integrated model of information systems adoption in small businesses. Journal of management information systems 15(4), 187–214 (1999)
34. Tornatzky, L.G., Fleischer, M., Chakrabarti, A.K.: Processes of technological innovation (1990)
35. Wästlund, E., Angulo, J., Fischer-Hübner, S.: Evoking comprehensive mental models of anonymous credentials. In: Open Problems in Network Security, pp. 1–14. Springer (2012)
36. Zafarani, R., Liu, H.: Connecting users across social media sites: a behavioral-modeling approach. In: The 19th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining, KDD 2013, Chicago, IL, USA, August 11-14, 2013. pp. 41–49 (2013)
37. Zhu, K., Dong, S., Xu, S.X., Kraemer, K.L.: Innovation diffusion in global contexts: determinants of post-adoption digital transformation of european companies. European Journal of Information Systems 15(6), 601–616 (2006)