Privacy-ABCs as a Case for Studying the Adoption of PETs by Users and Service Providers

Ioannis Krontiris[3(✉)], Zinaida Benenson[1], Anna Girard[1], Ahmad Sabouri[2], Kai Rannenberg[2], and Peter Schoo[3]

[1] Friedrich-Alexander-University Erlangen-Nuremberg, Erlangen, Germany
zinaida.benenson@cs.fau.de, anna_girard@hotmail.de
[2] Goethe University Frankfurt, Frankfurt, Germany
{ahmad.sabouri,kai.rannenberg}@m-chair.de
[3] European Research Center, Huawei Technologies, Munich, Germany
{ioannis.krontiris,peter.schoo}@huawei.com

Abstract. Although in the last years there has been a growing amount of research in the field of privacy-enhancing technologies (PETs), they are not yet widely adopted in practice. In this paper we discuss the socioeconomical aspects of how users and service providers make decisions about adopting PETs. The analysis is based on our experiences from the deployment of Privacy-respecting Attribute-based Credentials (Privacy-ABCs) in a real-world scenario. In particular, we consider the factors that affect the adoption of Privacy-ABCs as well as the cost and benefit trade-offs involved in their deployment and usage, as perceived by both parties.

1 Introduction

Safeguarding privacy is vital for building trust in the online environment and facilitating economic development. It is important to show to citizens that going online is not just convenient, but also trustworthy and that their data won't be mismanaged or misused, sold or stolen. To strengthen trustworthiness in the online environment in a practical and effective way, "privacy by design" is becoming an essential principle, meaning that data protection safeguards should be built into products and services from the earliest stage of development.

One way of realizing privacy by design is by using Privacy-Enhancing Technologies (PETs). During the last years, there is a growing amount of research in the field of PETs enabled by major advances in cryptography. They provide advanced privacy features such as anonymous protection of real-time communication, privacy-respecting identity management and methods for anonymously retrieving online content.

Yet, PETs are not widely adopted in practice so far [16]. One cannot expect a simple explanation to this, as online privacy is a complex and interdisciplinary issue. Several of the technical aspects have been addressed at a satisfactory

B. Berendt et al. (Eds.): APF 2015, LNCS 9484, pp. 104–123, 2016.
DOI: 10.1007/978-3-319-31456-3_6

degree, but there are still several socioeconomical aspects of PETs adoption that only now begin to draw attention. In this paper we discuss in particular the cost-benefit trade-offs involved in adopting such technologies, as perceived by both users and service providers.

In 2010, the European Commission sponsored a study of the economic costs and benefits of PETs [15], which shows clearly that costs and benefits are technology specific as well as dependent on the applications in which PETs are deployed. Therefore, in this paper we narrow down the discussion by focusing on a specific PET and on a particular application scenario. More specifically, during the last four years, the EU-funded research project ABC4Trust[1] concentrated on the advancement of Privacy-respecting Attribute-based Credentials (Privacy-ABCs) and its applicability in real-world scenarios. In this paper we report our experiences from working within this project and especially our analysis from one of the user trials.

In the first part of the paper we explore the adoption of Privacy-ABCs from the users' side. Which factors influence their intention to use such tools and how do they perceive the trade-off between benefits and costs connected with the usage? User acceptance of advanced PETs had rarely been studied outside the laboratory, and so we are one of the first to present such results. In the second part of the paper we discuss the factors that might affect the adoption of Privacy-ABCs by service providers. In deciding whether to invest in PETs, service providers engage in a cost-benefit trade-off involving many factors related not only to internal processes and business models but also to the external environment, such as legislation, user demand or global infrastructure readiness.

2 The Privacy-ABCs Case

Providing privacy in the identity management area means moving towards a claims-based architecture [9]. In this kind of architecture, the service provider publishes a *Policy* on accessing a specific resource and expects to receive claims from trusted sources that satisfy this policy. The trusted sources that issue such security tokens are the identity service providers (IdSP), sometimes also called identity providers for simplicity. An important characteristic of claims-based architecture is the separation between service providers and IdSPs, so that there is no direct exchange of information between them. Instead, the user resides in the middle, having control over the exchange of his identity information.

Claims-based architectures can use privacy-respecting credential systems (i.e., Privacy-ABCs) to provide untraceability and minimal disclosure. Examples of such credential systems are Idemix [8] and U-Prove [7]. Over the last few years, Idemix and U-Prove have been developed to offer an extended set of features, even though these features are named differently and they are realized based on different cryptographic mechanisms. In 2010, the EU research project ABC4Trust was initiated with the goal to alleviate these differences and unify

[1] https://abc4trust.eu/.

the abstract concepts and features of such mechanisms. Privacy-ABCs are privacy respecting credentials that are defined over these concepts and features and are independent from the specific cryptographic realization beneath.

One of the main achievements of ABC4Trust project was to test Privacy-ABCs in real-world situations within the scope of two large-scale user trials. This gave us valuable experiences regarding the interaction of users and system designers with the technology. More specifically, one of the user trials was conducted at Patras University in Greece, the results of which we present here.

The main goal of the user trial in Patras was to enable university students to login onto an online evaluation system at the end of the semester and evaluate the courses they attended, remaining anonymous to the system. At the same time, the system had to guarantee that only eligible students have access to the evaluation of a course. That is, the system had to first verify that a student (1) had registered to the course and (2) had attended most of its lectures.

To be able to prove the they satisfy the above conditions, students collected Privacy-ABCs and stored them in smartcards that they had been provided with. Specifically, they collected two credentials from the university, one for being enrolled as students at the institution and one for being registered for the specific course. During the semester, they obtained an attendance unit (implemented as increasing a counter value) per lecture by waving their smartcard in front of a contactless reader at the end of the lecture.

At the end of the semester, the students could use their smartcards to login anonymously at an online Course Evaluation System (CES) and fill the course evaluation form. During the authentication process, the students were first presented with the Policy of the CES at the user interface. Then they could select different attributes from their credentials and produce a presentation token corresponding to this policy and in that way authenticate to the CES, revealing only the minimum required information.

Privacy-ABCs are an attractive solution for the course evaluation scenario, priviging advantages for students as well as for the lecturers. On the one hand, students don't reveal their identity to the CES, but present themselves under a random pseudonym. Moreover, the CES cannot link the evaluations of two different courses back to the same student. On the other hand, privacy-ABCs assure that only students that actually attended a specified amount of lectures are able to evaluate the course. Students can evaluate each course only once and when they do so a second time, the new evaluation replaces the old one.

3 User Acceptance of Privacy-ABCs in a University Course Evaluation

The user trial in Patras gave us a unique opportunity to study the reactions of users while they interacted with the Privacy-ABC technology and get an empirical understanding of the factors that influence user acceptance of Privacy-ABCs. Below we present our findings and discuss lessons learned from the trial about the trade-offs between the benefits of Privacy-ABCs and the costs perceived by

the users. More details on the trial organization can be found in the full report of the trial [29], whereas for the more specific details of the theoretical development and validation methodology we refer the interested reader to [4].

3.1 Theoretical Background and Methodology

Theoretical User Acceptance Factors for Privacy-ABCs. In order to investigate user acceptance factors of Privacy-ABCs, we first developed a theoretical model for possible acceptance factors, drawing from related work on general technology acceptance [10,24,34], as well as acceptance of security- and privacy-related technologies [18,28,30]. We identified possible user acceptance factors that are presented in Table 1 and will be explained below in more detail.

Table 1. Factors of user acceptance of Privacy-ABCs and their correlations to the intention to use Privacy-ABCs for course evaluations. m denotes the mean values for the corresponding scales, σ denotes standard deviations. For details on the measurement results, see Fig. 1. Correlation results are discussed in depth in Sect. 3.2.

Factor (psychometric scale)	Definition in the context of the Patras Privacy-ABCs trial	m	σ	Kendall's τ
Perceived Usefulness for the Primary Task	The degree of agreement that Privacy-ABCs are useful for course evaluation	4.10	0.66	0.726^{**}
Perceived Usefulness for the Secondary Task	The degree of agreement that Privacy-ABCs are useful for privacy protection	3.93	0.74	0.420^{**}
Perceived Ease of Use	The degree of agreement Privacy-ABCs usage is free of effort	3.83	0.65	0.498^{**}
Perceived Risk	The degree of agreement that course evaluation using Privacy-ABCs is risky	1.80	0.99	-0.444^{**}
Trust	The degree to which the Privacy-ABC System is perceived to be trustworthy	4.13	0.73	0.326^{*}
Situation Awareness	The perception of being well informed about what is going on in the system	3.87	0.63	0.319^{*}
Understanding of the Technology	The ability to correctly answer questions about the key aspects of Privacy-ABCs	0.51	0.45	0.065

Significance levels: * $p < 0.05$; ** $p < 0.01$
Correlation strength: $0.1 < \tau \leq 0.3$ weak, $0.3 < \tau \leq 0.5$ moderate, $\tau > 0.5$ strong

Considering the general technology acceptance, the most influential theoretical model is *Technology Acceptance Model (TAM)* [10,32,33], that has been later

extended to the *Unified Theory of Acceptance and Use of Technology (UTAUT).* Although UTAUT [34] and its recent extension UTAUT2 [35] are more successful models than TAM in predicting technology acceptance, we identified TAM as being more suitable in the context of the Privacy-ABC trial (see Appendix A for an in-depth discussion). In a nutshell, as we knew the demographic characteristics of our participants in advance, we could predict from the existing literature and from out previous experience with Privacy-ABCs [5] that testing additional UTAUT and UTAUT2 factors would not be possible and would only overload the (already very substantial) questionnaire.

TAM considers *Perceived Ease of Use* and *Perceived Usefulness* of a technology as main factors in user acceptance, while user acceptance is conceptualized as intention to use the technology in the future. However, security- and privacy-enhancing technologies rarely serve *primary* user goals, such as communication or online shopping. They are expected to work in the background, protecting the user and thus facilitating the successful execution of the primary task. Therefore, we decided to distinguish between *Perceived Usefulness for the Primary Task* (i.e., the course evaluation) and *Perceived Usefulness for the Secondary Task* (i.e., the privacy protection during the course evaluation). *Perceived Ease of Use* did not need any special adaptation.

Security- and privacy-sensitive scenarios usually involve perceived risk and trust as factors of user participation. User's assets (such as data, money or reputation) can be put at risk, and the decision to participate in such a scenario involves risk assessment and depends on the trust in other parties and in the underlying technology. Pavlou [24] integrated trust and perceived risk into the TAM in the context of online shopping. Building on his work, we consider *Trust* into the Privacy-ABC technology and *Perceived Risk* of usage of the Privacy-ABC technology as important acceptance factors.

Trust is defined as "beliefs that a specific technology has the attributes necessary to perform as expected in a given situation in which negative consequences are possible" [21, p. 7]. We note that users' expectations from the technology in the context of the trial refer not only to privacy protection during the course evaluation, but also to other properties of the course evaluation system that is implemented using Privacy-ABCs, such as reliable collection of course attendance credentials or error-free storage and processing of the course evaluation results.

Spiekermann [28] investigates situation awareness as a possible factor that drives adoption of privacy-enhancing technologies for RFID. Building on her research, we consider this factor in our investigation as well. *Situation Awareness* is defined as "personal perception to be informed about what is going on" [28, p. 134]. In connection with Privacy-ABCs, Situation Awareness includes knowing which information will be disclosed in order to get a credential, who receives the data, which data is stored on the smart card, etc.

Usually, people do not need to understand exactly how a technology works in order to be able to use it. Much more important than the exact understanding is the development of a *mental model* of the technology that enables correct usage.

Mental models are representations of reality in people's minds, their conceptions about how things work. As discovered by Wästlund et al. [36], correct mental models of Privacy-ABCs are especially difficult to convey.

Although expert technical knowledge might not play an important role in user acceptance, *misunderstanding* of some key concepts could result in poor adoption. For example, Sun et al. [30] discovered that some users think that their login credentials are given to every participating party when they use single sign-on, which lead to (wrongly) perceived additional insecurity, and thus to unwillingness to use the technology. Therefore, we investigate *Understanding of the Technology* as a possible factor of user acceptance.

Methodology for Validation of User Acceptance Factors. In order to assess the relative importance of the user acceptance factors, we developed a quantitative standardized questionnaire that the participants filled in shortly after the course evaluation deadline. In this way, they were able to assess all available functions of the Privacy-ABC System, such as credentials collection, backup of the smartcard data and course evaluation.

We developed Likert scales [14] for all constructs presented in Table 1, apart from *Understanding of the Technology* that was assessed by means of a knowledge quiz. Each scale consists of several statements, called items. The users rated the items from 1 = "strongly disagree" to 5 = "strongly agree". The scales are presented in Appendix B. All developed multi-item scales fulfill the following quality criteria: one-dimensionality (Kaiser-Meyer-Olkin criterion > 0.5, total variance explained $> 50\,\%$) and reliability (Cronbach's $\alpha > 0.7$) [14]. More details on scale construction and quality criteria are presented in [4].

Participants. 30 out of 45 participants of the Patras trial answered our questionnaire and so all further analyses relate to the sample size of 30 subjects (23 male, 7 female, 23 years old on average).

The participants are active Internet users: 25 participate in online social networks, 23 shop online, and 17 use online banking. 26 participants expressed a high or very high level of Internet privacy concerns ($m = 4.03$, $\sigma = 0.86$)[2] on a 5-point Likert scale developed by Dinev and Hart [12]. Most participants exhibit privacy-aware behavior: more than two thirds said that they at least sometimes delete cookies, clean browser history, use their browser in private mode and provide fake information when creating a web account. However, only three participants ever used a PET before (TOR in all cases).

Participation in course evaluations was reported as being important or very important by 21 participants, and 28 participants indicated that protection of anonymity during course evaluations is important (9) or very important (19) for them, with the remaining two participants reporting a neutral attitude.

[2] m denotes mean value, σ denotes standard deviation.

3.2 Results on User Acceptance Factors

Descriptive Statistics. The measurements for the user acceptance factors[3] are presented in Fig. 1. Overall, the Patras users found Privacy-ABCs useful, trustworthy, and usable. The positive evaluation results are mirrored by the high level of intention to use Privacy-ABCs for course evaluation in the future: 29 out of 30 users expressed this intention. Comparing the Privacy-ABC System with the paper-based course evaluation that is usually conducted at their university, 28 participants indicated that they prefer using a Privacy-ABCs-based system over a paper-based system.

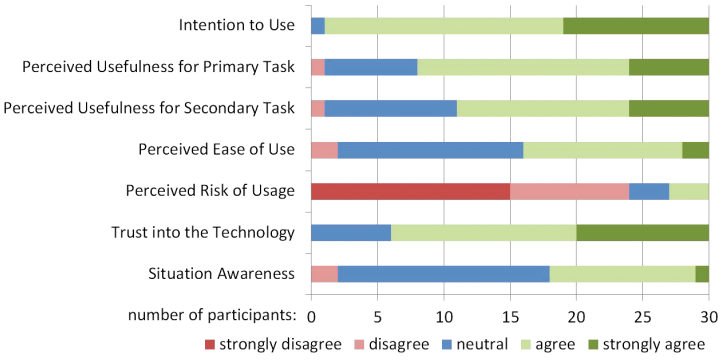

Fig. 1. Measurements of intention to use and acceptance factors.

Considering the results in more detail, more than two thirds of the users (22) perceived Privacy-ABCs to be useful for course evaluation (primary task), and 19 users found Privacy-ABCs to be useful for privacy protection (secondary task) as well. 14 participants found the system easy to use, with additional 14 participants expressing a neutral usability attitude. Participants expressed a low level of risk perception and a high level of trust into the system: cumulatively, 24 users (80 %) disagreed or strongly disagreed with the system usage being risky, and agreed or strongly agreed with the system being trustworthy. Finally, 12 users agreed that the Privacy-ABC system provides a good overview of what happens during the usage (Situation Awareness), with additional 16 users demonstrating a neutral attitude.

Statistical Correlations. In order to understand in more detail the relation between the acceptance factors and the intention to use Privacy-ABCs, we explored statistical correlations between the acceptance factors and the reported intention of the participants to use Privacy-ABCs for course evaluations in

[3] Understanding of the Technology factor will be discussed later in Sect. 3.3 for readability reasons.

the future. We conducted bivariate non-parametric two-tailed correlations using Kendall's correlation coefficient (τ). This test does not require normal data distribution and works for ordinal data and small sample sizes. We report the results in Table 1. The correlation coefficient τ indicates the strength of the association between the variables, whereas the significance level $p < x$ means that the probability of the corresponding correlation to occur by chance is less than x.

Ease of Use, both kinds of Perceived Usefulness, Trust and Situation Awareness are significantly positively correlated to the intention to use Privacy-ABCs for the course evaluations, whereas Perceived Risk is significantly negatively correlated. The correlation coefficients are medium for all correlations except for Perceived Usefulness for Primary Task with the large effect size (0.726), which points at this factor as the most important one for user acceptance.

Quite surprisingly, there is no correlation between the understanding of Privacy-ABCs and the intention to use them, although we would have expected some connection. For example, people who understand the pseudonymization properties of Privacy-ABCs especially well might had felt more inclined to use them, or people who misunderstand some Privacy-ABCs' properties might had felt averse towards Privacy-ABCs usage. In the next section, we discuss the understanding of Privacy-ABCs in more details.

3.3 Understanding of Privacy-ABCs

The participants in the Patras trial have high technical literacy and were given an introductory lecture on the topic of Privacy-ABCs properties. Nevertheless, the understanding of fundamental properties of the system turned out to be unexpectedly low. We measured how well the participants understand the concepts behind the Privacy-ABCs by means of a knowledge index consisting of five statements that could be rated as true or false, with the "don't know" answer option also available. Due to space limitations, we discuss only the most important results here, more details are available in [4,29].

The participants expressed a low level of understanding of the pseudonymization property of Privacy-ABCs: Only 14 participants rightly stated that their matriculation number (a unique identifier) is not transmitted to the Course Evaluation System during the authentication process. Considering the weak understanding of Privacy-ABCs, the high level of perceived usefulness of Privacy-ABCs for privacy protection (Fig. 1) seems to be non-rational.

Even less participants (11) rightly indicated that the number of their class attendances (a potentially identifying and unnecessary piece of information) is not transmitted when they evaluate the course. Actually, only the fact that a student attended more than half of the course's lectures is disclosed to the system, which qualifies the student to evaluate this course.

These results indicate that users' perception to be well informed about what is happening in the system (Situation Awareness) and the overall high level of trsut into the system may be more important than the actual understanding of the system.

3.4 Cost-Benefit Trade-Offs in User Acceptance

From the economics point of view, user acceptance of a technology is tightly connected to a (sometimes unconscious) cost-benefit assessment of the technology [2,13]. We directly assessed the perceived cost-benefit relation by asking the users to rate their corresponding perception. 23 participants agreed or strongly agreed that the benefits outweigh the costs, additionally 6 participants showed a neutral attitude, and one participant disagreed.

The benefits of Privacy-ABCs can further be expressed in terms of their perceived usefulness. Most participants found the system useful for course evaluations as well as for privacy protection, as discussed previously.

The costs of the Privacy-ABCs in the Patras trial are mostly incurred by usability issues. According to users' ratings of the Perceived Ease of Use presented in Fig. 1, the usability costs were perceived as relatively low. Additionally, we also examined the usability costs in more detail. We asked the participants to rate statements about concrete usability characteristics of the system:

- *Mental effort:* Interaction with the Privacy-ABC system requires a lot of mental effort
- *Physical effort:* Interaction with the Privacy-ABC system takes too much time for manual operations (for example clicks, data input, handling the smart card)
- *Learnability effort:* Usage of the Privacy-ABC system is difficult to learn
- *Memorability effort:* Remembering how to interact with the Privacy-ABC system is difficult
- *Low helpfulness:* Help information provided by the the Privacy-ABC system is not effective
- *Error recovery effort:* Mistakes made during the Privacy-ABC system usage are difficult to correct
- *Worries about smartcard loss:* Users' anxiety about the possibility of losing his/her smartcard
- *Uneasiness about data on smartcard:* User feels uncomfortable knowing that his/her personal data is saved on a smartcard

As can be seen in Fig. 2, the incurred costs are mostly perceived as low, e.g., only 5 participants found that the system usage requires physical effort, and 3 participants found the system difficult to learn. The only "expensive" task was remembering how to interact with the system (5 participants found this easy to do). We hypothesize, however, that high system helpfulness (22 participants disagreed or strongly disagreed with the low helpfulness of the system) and good error recovery probably mitigated this disadvantage.

We conclude that users' perception that the PET usage does not require a lot of physical and mental effort, and the resulting positive cost-benefit assessment of the Privacy-ABC technology might play an important role in user acceptance. Moreover, some usability costs (such as low memorability) can be compensated by other, more usable features.

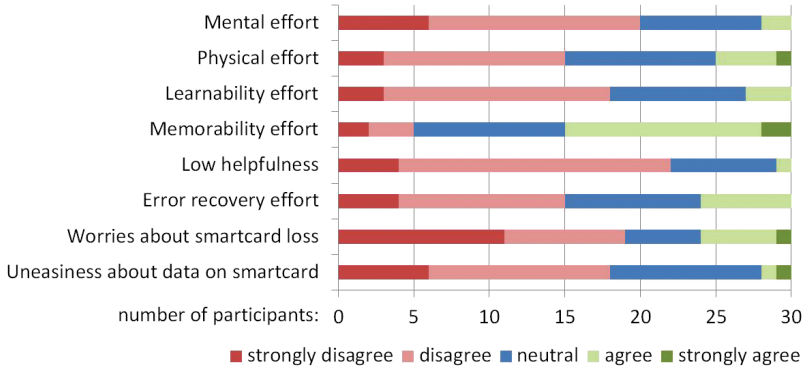

Fig. 2. Usability costs of Privacy-ABCs usage in the course evaluation.

We note, however, that it is impossible to draw causal conclusions from our trial. Did the high system usability influence perceived usefulness and users' high intention to use the system in the future? On the contrary, probably the high perceived usefulness of the system influenced user's positive usability perceptions. More research is needed to answer these questions.

3.5 Limitations of the Study Results

The results of the Patras pilot have to be further verified in other studies, as our trial had a lot of limitations that might have influenced the results. For example, users that found Privacy-ABCs inconvenient or untrustworthy could have refused to participate (so-called self-selection bias), such that we were unable to investigate their opinions and technology rejection factors.

Furthermore, the trustworthy university environment could have increased trust into the system, and thus also the perceived usefulness for privacy protection. Moreover, computer science students are more likely to be early adopters, which could imply exaggerated user acceptance results in comparison to the general population. Also good usability results may have been positively influenced by the high technical literacy of the users.

3.6 Promoting PETs Usage by the End Users

According to the conventional wisdom, in order to adopt PETs, people need to understand their benefits. It is also often assumed that risk perception is connected to the understanding of privacy risks. The reasoning is that if the users would perceive risk for their privacy as high, and the efficacy of PETs in reducing this risk as high, then they would adopt PETs. However, we see a different picture in our trial. Although the participants did not understand the properties of Privacy-ABCs well, they expressed a high level of trust into the system. Moreover, their perception of the overall system as useful for the primary

task is strongly correlated with high user acceptance. While the usefulness of Privacy-ABCs for privacy protection and the usability of the system are important acceptance factors, the most important factor of user acceptance turned out to be the usefulness of Privacy-ABCs for the service (course evaluation) in which they were integrated.

We conclude with a tentative suggestion: Integration of sophisticated PETs into systems and products should be driven by political, legal and ethical considerations, not by user demand, as there are too many impediments for the latter. These impediments are well known from the behavioral economics: incomplete information, bounded rationality and behavioral biases [3].

We could observe the influence of these impediments in our trial: The participants trusted the system despite their low understanding of its properties, and expressed the wish to use it because they perceived the system as useful for the task that is important for them (course evaluation). Especially interesting is that these results were obtained for technically savvy and privacy-aware users.

Therefore, our results may also be valid for general Internet population. We think that the users would only adopt PETs that are integrated into useful services. In this case, we think that people may accept some usability drawbacks that arise from the PET integration, such as having to use a smart card or to consult a user manual sometimes. Although good usability and usefulness for privacy protection are important factors of user acceptance, our empirical results indicate that perceived usefulness of the primary (not privacy-related) service is much more important.

4 Adoption of PETs by Service Providers

For many PETs, like Privacy-ABCs, adoption from the users is not enough, but they rather require that service providers also support their use from their side. In this regard, the results of an expert survey [27] investigates the factors that may become a driver or an inhibitor for service providers' decision to adopt such kind of PETs in their processes. In this section we give an overview of the relevant factors and report our experiences from the Patras pilot, wherever appropriate.

4.1 Which Factors of Acceptance to Consider?

The literature in Information Systems research provides a handful list of theories explaining adoption of new innovations. From the prominent ones that have been verified by various empirical studies, four theories that focus on the organizational level of technology adoption [11,19,25,31] could be combined into a single conceptual model to highlight the factors influencing adoption of technologies like PETs. Below we discuss in more details the resulted set of factors, which we have grouped into five categories.

Technology. Most PETs are newly introduced technologies and their characteristics may have a strong influence on the decision of the potential adopters.

Compatibility. It refers to the degree to which an innovation is perceived as consistent with the existing values, needs, and past experiences of the potential adopters. Therefore, higher compatibility of PETs' specification with the existing protocols and standards that are commonly used would support the adoption.

Complexity. It refers the degree to which an innovation is perceived as relatively difficult to understand and use. For example, Privacy-ABCs are based on difficult cryptographic concepts, which are not easy for people beyond the cryptographers to understand. In this regard, further effort to provide the policy makers and application developers with supporting materials facilitating their understanding as well as developing better user-interfaces for the end users seems to be crucial.

Trialability. It is defined as the degree to which an innovation may be experimented and tested on a limited basis. In other words, it concerns how easy it would be for a potential adopter to test (or partially test) the features that the new technology provides. This concern exists for example among the scientific community around Privacy-ABCs, as they have been constantly developing and publishing supporting-materials such as reference implementation and online resources to facilitate examining Privacy-ABCs.

Observability. It refers to the extent to which the innovation or its results are visible to the others. Unlike many other innovations that have visible results and can be well demonstrated, some PETs like Privacy-ABCs are very challenging to present. They are not like stand-alone products or services, but instead they are integrated into those. Therefore, demonstrators have difficulties showing all the added values of PETs in demos.

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. This is in general necessary for adopting a new technology. Concerning PETs, top management's attitude towards changes caused by PETs can influence their adoption.

Business Dependency on User Data Collection. Dependency of the organization's business model on the collection of excessive personal data can negatively influence adoption of PETs like Privacy-ABCs, as some of these technologies are built to reduce the amount of collected personal data only to the minimum necessary.

Technology Competence. Our experience from the ABC4Trust pilots shows that typical developers often have difficulties to integrate Privacy-ABCs into services on their own, and constant support of technology providers would be needed. At the same time developers with scientific background and technical understanding of the technology went through the integration process smoothly. Hence, lack of technical competency can hinder PETs adoption.

External Pressure. Various sources of external pressure may influence the adoption of new innovations and in particular PETs.

Regulatory Pressure. A regulatory body may be the source of coercive pressures [26]. The regulations may directly address privacy and require the business to implement privacy enhancing mechanisms, or they may indirectly touch the topic, for instance by defining more costly requirements to protect the collected personal data.

Social Pressure. There have been major incidents recently, which we expect to have an influence on the adoption of PETs in general. The most well-known incidence was brought up by Edward J. Snowden, 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 service providers will increase and push them towards employing mechanisms that reduce personal data collection in their processes.

Extent of Adoption among Competitors. Knowing a competitor has adopted an innovation and it has been a success, a firm tends to adopt the same innovation. We also consider that adoption of PETs by the competitors of a firm motivates it to follow the same approach not to lose trust.

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.

Environment. Here we refer to the external conditions that do not introduce any pressure, but they 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. Having the already established infrastructure ready to support PETs, the integration of these technologies into the platforms of service providers could become less costly and more attractive. Let us take eIDs as an example, which have been implemented in various countries around the world. Service providers can benefit greatly from the established infrastructure to perform authentication and access control in their online businesses. It is important that PETs, like Privacy-ABCs, can be integrated with the existing eID infrastructure without requiring any modifications to this infrastructure [6]. The EU Project FutureID[4] is studying in depth how such an integration can be done to take full advantage of Privacy-ABCs.

[4] http://futureid.eu.

Perceived Benefits and Costs. There are several factors not included in the four categories above and which encompass monetary benefits but also costs, obligations and potential lost revenue. The trades-off and the resulting monetary effects are discussed separately in Sect. 4.3.

4.2 Influence Level of the Factors

The aforementioned factors have been formulated into a questionnaire targeting experts from various relevant domains in order to collect their opinion on the influence level of these factors on the adoption of Privacy-ABCs [27]. The statistical results demonstrate that the experts considered *Business Model Dependency to Data Collection*, *Complexity for User*, *Observability*, *Top Management Support*, *Trialability*, *Cost of Integration*, *Complexity for Developers*, and *Regulations for Data Collection* as the top 8 most important or influential factors impacting the decision of the service providers to employ Privacy-ABCs.

4.3 Cost-Benefit Trade-Offs

Here costs can be seen as investments, but also potentially lost revenue from a risk analysis point of view. Likewise, benefits can be seen as reducing liabilities and costs, but also gaining reputation and new users.

The Costs of PETs for Service Providers. Certainly, several of the factors that affect service providers' decision to adopt a specific PET are related to the financial aspects around the collection of personal data. Currently service providers benefit from the collection of excessive personal data that allows them to personalize advertisement of goods and services and also improve new ones. For example, price discrimination or targeted advertising is based on such data, while the whole realm of big data today is based on the principle of collecting as much data as possible and find use of this data later.

This holds especially for big data categories *analysis* and *predict & project*, where it is assumed that the quality of data analysis will increase over time. Thus history information has a specific high value. For personal data this can in turn be harmful. Consent to use their personal data was given by end users not being able to identify at time of agreement those analysis, prediction, or projection methods that could be used in the future. For these big data categories suitable PETs will be extremely helpful.

In these lines, if PETs diminish the usefulness of personal data, this could be seen as a cost associated with their deployment. However, this is not always the case and PETs may make it possible to reach a new economic equilibrium where data holders can still profit from the value of data, while subjects' individual information stays protected. For example, Acquisti has argued that using PETs like Privacy-ABCs is compatible with price discrimination strategies [1].

There is also a social loss associated with the uncertainty created to users about the deployment of PETs at the service provider, as usually service

providers do not reveal details about the level of protection offered. However, sometimes the quality of data protection is certified by seals that 3rd parties testified, which can help mitigate the problem.

Another kind of costs is related to the investment costs for the integration and deployment of PETs inside the service provider. The implementation of several PETs is now available as an Open Source Software (including Privacy-ABCs[5]), but their integration to a specific service or product can still require a lot of effort. This was experienced in the case of the Patras pilot, where the adaptation of the core reference implementation to the specific scenario took considerable effort, with additional complexity introduced by the use of smart cards and the enhancements regarding the revocation and inspector services. In general, there is lack of engineering techniques that would facilitate the smooth integration of PETs and only recently this area has started to attract interest[6].

Furthermore, investment can become especially troublesome in cases of international companies that operate worldwide and need to conform their services to different standards and privacy regulations. This was experiences in a smaller scale within ABC4Trust, where one partner company had the role of data processor developing part of the system and University of Patras had the role of data controller. To minimize the contact of the former with personal data kept by the latter, a step-by-step procedure with several safeguards had to be established through a legal contract, which limited the flexibility of the data processor [17].

Finally, sometimes the service provider might need to educate the users about the usage of a new PET, which can also be considered as a cost. We saw this in the Patras user trial, where the University gave to the students an introduction to Privacy-ABCs before they start using it and it distributed an extensive user manual about the system. During the user trial, the students requested additional support sending in total more than 150 emails to the support team, mostly regarding problems with the use of smart cards.

The Benefits of PETs for Service Providers. One of the benefits for using PETs is the limitation concerning the liabilities and costs due to lost or misused personal data. Indeed, one privacy risk that service providers face today is related to insufficient protection of personal data that are collected and stored by them. For example the insufficient deletion of personal data and the insufficient response to data breaches can have huge financial consequences to the company. There have not been reliable estimates of the potential loss from a privacy incident, but according to the upcoming EU data protection reform, data protection authorities will be able to fine companies that do not comply with EU rules with up to 2 % of their global annual turnover[7]. So from a risk management point of

[5] https://github.com/p2abcengine/p2abcengine.

[6] E.g., see the Internet Privacy Engineering Network initiative (https://secure.edps.europa.eu/EDPSWEB/edps/EDPS/IPEN).

[7] http://europa.eu/rapid/press-release_MEMO-14-186_de.htm last visited May 15th, 2015.

view, handling personal data can become very costly and using PETs can help address these risks.

Another aspect that promotes investments in PETs is the concerns about the harms in reputation associated with high-profile privacy incidents, which is expected to have a bigger impact as regulation is becoming stricter in mandating disclosure of privacy failures. Even though is has been suggested that firms lose billions of dollars due to privacy concerns, there are still not clear data to support this. An aspect to be considered here is how consumers' behavior is affected after privacy breach notifications, given that people's intentions with regard to privacy differ from their actual behavior [22].

An indirect but important benefit from PETs is that they can help service providers save costs by decreasing the risk of fraud or by protecting the organization's trade secrets. For example, in the identity management ecosystem it can be a competitive threat, if IdSPs learn all the users of the service providers. The use of Privacy-ABCs prevent this by placing the user between IdSPs and service providers.

5 Concluding Remarks

The results of the Patras trial indicate that users may not need to understand a PET in order to use it, as long as they trust the technology. The most important acceptance factor is the usefulness of the technology for the service they want to access, leaving ease of use (usability) to play a less important, but still significant role. Overall the benefits of Privacy-ABCs for the users overtook the costs.

Although the participants of the trial are not representative for the general Internet population, these results may still be generalizable, as the Patras pilot was conducted with the users that had probably the best possible chances and the best incentives for understanding Privacy-ABCs: technically savvy and privacy-aware computer science students.

For the service providers, economic forces, cryptographic technologies, and targeted regulatory guidelines would have to conspire to lead to adequate adoption. This is what Laudon called "co-regulative" solutions to privacy problems [20]. But the right balance will be decided from a societal viewpoint and may thus be different from society to society.

Looking to the future, we are still missing more and broader field trials to explore the socioeconomic factors of privacy technologies. There are some EU-wide surveys on public perception of privacy (e.g., [23]), but more focused ones on the adoption factors of PETs is still missing. Moreover, we should investigate not only adopters, but also non-adopters of PETs in order to better understand the acceptance factors. We are also especially missing controlled user acceptance experiments that would shed light on the causal relation between the user acceptance factors.

From the service providers' point of view, firms are more likely to utilize cost-benefit analysis if there is reliable data to inform the analysis. Until today however we are still missing large-scale data. For example, there have not been

reliable estimates of the potential loss from a privacy incident. Also there is little data on the reputation impact of privacy breach notifications or on the revenue loss of firms due to privacy concerns.

A Discussion on the Applicability of UTAUT and UTAUT2

Although UTAUT [34] and UTAUT2 [35] are more successful models than TAM in predicting technology acceptance, we identified TAM as being more suitable in the context of the Privacy-ABC trial.

TAM considers two main factors that influence user adoption: Perceived Usefulness (called Performance Expectancy in UTAUT) and Perceived Ease of Use (called Effort Expectancy in UTAUT). UTAUT extends TAM with one additional factor that directly influences intention to use the technology: Social Influence, which is the degree to which the user perceives that people whose opinion the user values believe that the user should use the technology.

We tested the influence of this factor in the first Privacy-ABC trial [5] and found no relation to the intention to use Privacy-ABCs. Therefore, we decided to drop this factor. We hypothesize that in the trial environment, this factor may not be applicable, as Privacy-ABCs are only known to the fellow students, and the usage in our scenario did not involve peer pressure (as this would be the case, for example, for social media).

These findings are consistent with the UTAUT and UTAUT2 investigations, where Social Influence was not found to be an important adoption factor, especially for younger users with high experience, as in our sample. We note, however, that for application of Privacy-ABCs in other scenarios and with other (older and less experienced) user populations, Social Influence may be considered.

Additionally, UTAUT considers some factors (age, gender, experience, voluntariness of use) that moderate the relation between the intention to use the systems and the main factors. Considering these moderators does not make sense in our case, however, as our sample is very homogeneous in this respect: The students are of very similar age and experience, all of them use the system voluntarily, and the overwhelming majority is male.

Similar non-applicability considerations apply to the UTAUT2 model that considers additional main acceptance factors: hedonic motivation (the user derives fun or pleasure from using the system), price value (the monetary cost of the system usage), and the habit in using the system.

B Measurement Scales for User Acceptance Factors

The constructs considered in this research are presented in Table 2 on page 18.

Table 2. Measurement scales for the user acceptance factors; all items were measured on a 5-point scale ranging from 1 = "strongly disagree" to 5 = "strongly agree".

Intention to Use (adpated from [32,33])
Assuming that the Privacy-ABC system is available for course evaluations, I intend to use it
I would use the Privacy-ABC system for course evaluations in the next semester if it is available
Given that the Privacy-ABC system is available for course evaluations, I would use it
Perceived Usefulness for Primary Task (adapted from [32,33])
Using Privacy-ABCs improves the performance of course evaluation
Using Privacy-ABCs enhances the effectiveness of course evaluation
I find Privacy-ABCs to be useful for course evaluation
Perceived Usefulness for Secondary Task (adapted from [32,33])
Using Privacy-ABCs improves my privacy protection
Using Privacy-ABCs enhances the effectiveness of my privacy protection
I find Privacy-ABCs to be useful in protecting my privacy
Perceived Ease of Use (adapted from [32,33])
Interacting with the Privacy-ABC System does not require a lot of my mental effort
The Privacy-ABC System is easy to use
I find it easy to get the Privacy-ABC System to do what I want to do
Perceived Risk (adapted from [24])
I would see the decision to evaluate the course with the Privacy-ABC System as a risky action
Trust into the Privacy-ABC technology (adapted from [24])
The Privacy-ABC System is trustworthy
Situation Awareness (adapted from [37])
With Privacy-ABCs, I always know which personal information I am disclosing
I find it easy to see which information will be disclosed in order to get a credential
Privacy-ABCs let me know who receives my data
The Privacy-ABC system gives me a good overview of my personal data stored on my Smart Card
I can easily find out when (e.g., at which date) I have received a credential via the University Registration System
I get a good overview of who knows what about my private information from the Privacy-ABC System
I can easily see which and how many Privacy-ABC credentials I have been issued

References

1. Acquisti, A.: Identity management, privacy, and price discrimination. IEEE Secur. Priv. **6**(2), 46–50 (2008)
2. Acquisti, A.: The economics of personal data and the economics of privacy. Background Paper for OECD Joint WPISP-WPIE Roundtable 1 (2010)
3. Acquisti, A., Grossklags, J.: Privacy and rationality in individual decision making. IEEE Secur. Priv. **2**, 24–30 (2005)
4. Benenson, Z., Girard, A., Krontiris, I.: User acceptance factors for anonymous credentials: an empirical investigation. In: Workshop on the Economics of Information Security (WEIS) (2015)
5. Benenson, Z., Girard, A., Krontiris, I., Liagkou, V., Rannenberg, K., Stamatiou, Y.: User acceptance of privacy-ABCs: an exploratory study. In: Tryfonas, T., Askoxylakis, I. (eds.) HAS 2014. LNCS, vol. 8533, pp. 375–386. Springer, Heidelberg (2014)
6. Bjones, R., Krontiris, I., Paillier, P., Rannenberg, K.: Integrating anonymous credentials with eIDs for privacy-respecting online authentication. In: Preneel, B., Ikonomou, D. (eds.) APF 2012. LNCS, vol. 8319, pp. 111–124. Springer, Heidelberg (2014)
7. Brands, S.: Rethinking Public Key Infrastructures and Digital Certificates: Building in Privacy. MIT Press, Cambridge (2000)
8. Camenisch, J., Van Herreweghen, E.: Design and implementation of the idemix anonymous credential system. In: Proceedings of the 9th ACM Conference on Computer and Communications Security (CCS 2002), pp. 21–30 (2002)
9. Cameron, K., Posch, R., Rannenberg, K.: Proposal for a common identity framework: A User-Centric Identity Metasystem. In: Rannenberg, K., Royer, D., Deuker, A. (eds.) The Future of Identity in the Information Society - Opportunities and Challenges. Springer (2009)
10. Davis, F.D.: Perceived usefulness, perceived ease of use, and user acceptance of information technology. MIS Q. **13**(3), 319–340 (1989)
11. DiMaggio, P.J., Powell, W.W.: The iron cage revisited: institutional isomorphism and collective rationality in organizational fields. Am. Sociol. Rev. **48**(2), 147–160 (1983)
12. Dinev, T., Hart, P.: Internet privacy concerns and social awareness as determinants of intention to transact. Int. J. Electron. Commer. **10**(2), 7–29 (2006)
13. Economics, L.: Study on the Economic Benefits of Privacy-enhancing Technologies (PETs): Final Report to The European Commission, DG Justice, Freedom and Security. London Economics (2010)
14. Field, A.: Discovering Statistics Using IBM SPSS Statistics. Sage, London (2013)
15. Final Report to the European Commission DG Justice, Freedom and Security: Study on the economic benefits of privacy-enhancing technologies (PETs). Technical report, London Economics, July 2010
16. Fischer-Hübner, S., Hoofnagle, C., Krontiris, I., Rannenberg, K., Waidner, M.: Online privacy: towards informational self-determination on the internet (Dagstuhl Perspectives Workshop 11061). Dagstuhl Manifestos **1**(1), 1–20 (2011)
17. Hansen, M., Bieker, F., Deibler, D., Obersteller, H., Schlehahn, E., Zwingelberg, H.: Legal data protection considerations. In: Rannenberg, K., Camenisch, J., Sabouri, A. (eds.) Attribute-based Credentials for Trust, pp. 143–161 (2015)
18. Herath, T., Chen, R., Wang, J., Banjara, K., Wilbur, J., Rao, H.R.: Security services as coping mechanisms: an investigation into user intention to adopt an email authentication service. Inf. Syst. J. **24**(1), 61–84 (2014)

19. Iacovou, C.L., Benbasat, I., Dexter, A.S.: Electronic data interchange and small organizations: adoption and impact of technology. MIS Q. **19**, 465–485 (1995)
20. Laudon, K.C.: Markets and privacy. Commun. ACM **39**(9), 92–104 (1996)
21. McKnight, D.H., Carter, M., Thatcher, J.B., Clay, P.F.: Trust in a specific technology: an investigation of its components and measures. ACM Trans. Manage. Inf. Syst. (TMIS) **2**(2), 12 (2011)
22. Nofer, M., Hinz, O., Muntermann, J., Roßnagel, H.: The economic impact of privacy violations and security breaches. Bus. Inf. Syst. Eng. **6**(6), 339–348 (2014)
23. Patil, S., Patruni, B., Lu, H., Dunkerley, F., Fox, J., Potoglou, D., Robinson, N.: Public perception of security and privacy: results of the comprehensive analysis of PACT's pan-european survey. Technical report, PACT EU Project Public Deliverable D4.2, June 2014
24. Pavlou, P.A.: Consumer acceptance of electronic commerce: integrating trust and risk with the technology acceptance model. Int. J. Electron. Commer. **7**(3), 101–134 (2003)
25. Rogers Everett, M.: Diffusion of Innovations. Free Press, New York (1995)
26. Rubinstein, I.S.: Regulating privacy by design. Berkeley Technol. Law J. **26**, 1409 (2011)
27. Sabouri, A.: Understanding the determinants of privacy-ABC technologies adoption by service providers. In: Proceedings of 14th IFIP WG 6.11 Conference on e-Business, e-Services, and e-Society, I3E 2015 Open and Big Data Management and Innovation, Delft, The Netherlands, 13–15 October 2015, vol. 9373 (2015)
28. Spiekermann, S.: User Control in Ubiquitous Computing: Design Alternatives and User Acceptance. Shaker, Aachen (2008)
29. Stamatiou, Y., Benenson, Z., Girard, A., Krontiris, I., Liagkou, V., Pyrgelis, A., Tesfay, W.: Course evaluation in higher education: the patras pilot of ABC4Trust. In: Rannenberg, K., Camenisch, J., Sabouri, A. (eds.) Attribute-based Credentials for Trust, pp. 197–239. Springer International Publishing (2015)
30. Sun, S.T., Pospisil, E., Muslukhov, I., Dindar, N., Hawkey, K., Beznosov, K.: What makes users refuse web single sign-on?: an empirical investigation of OpenID. In: Proceedings of the Seventh Symposium on Usable Privacy and Security, p. 4. ACM (2011)
31. Tornatzky, L.G., Fleischer, M., Chakrabarti, A.K.: Processes of Technological Innovation. Lexington Books, Lexington (1990)
32. Venkatesh, V., Bala, H.: Technology acceptance model 3 and a research agenda on interventions. Decis. Sci. **39**(2), 273–315 (2008)
33. Venkatesh, V., Davis, F.D.: A theoretical extension of the technology acceptance model: four longitudinal field studies. Manage. Sci. **46**(2), 186–204 (2000)
34. Venkatesh, V., Morris, M.G., Davis, G.B., Davis, F.D.: User acceptance of information technology: toward a unified view. MIS Q. **27**, 425–478 (2003)
35. Venkatesh, V., Thong, J.Y., Xu, X.: Consumer acceptance and use of information technology: extending the unified theory of acceptance and use of technology. MIS Q. **36**(1), 157–178 (2012)
36. Wästlund, E., Angulo, J., Fischer-Hübner, S.: Evoking comprehensive mental models of anonymous credentials. In: Camenisch, J., Kesdogan, D. (eds.) iNetSec 2011. LNCS, vol. 7039, pp. 1–14. Springer, Heidelberg (2012)
37. Wästlund, E., Wolkerstorfer, P., Köffel, C.: PET-USES: Privacy-enhancing technology-users self-estimation scale. In: Privacy and Identity Management for Life, pp. 266–274. Springer (2010)