User Acceptance of Privacy-ABCs: An Exploratory Study

Zinaida Benenson[1], Anna Girard[1], Ioannis Krontiris[2], Vassia Liagkou[3], Kai Rannenberg[2], and Yannis Stamatiou[2]

[1] Friedrich-Alexander-University Erlangen-Nuremberg, Germany
[2] Goethe University Frankfurt, Germany
[3] Computer Technology Institute Patras, Greece

Abstract. In this work, we present the first statistical results on users' understanding, usage and acceptance of a privacy-enhancing technology (PET) that is called "attribute-based credentials", or Privacy-ABCs. We identify some shortcomings of the previous technology acceptance models when they are applied to PETs. Especially the fact that privacy-enhancing technologies usually assist both, the primary and the secondary goals of the users, was not addressed before. We present some interesting relationships between the acceptance factors. For example, understanding of the Privacy-ABC technology is correlated to the perceived usefulness of Privacy-ABCs. Moreover, perceived ease of use is correlated to the intention to use the technology. This confirms the conventional wisdom that understanding and usability of technology play important roles in the user adoption of PETs.

Keywords: privacy enhancing technologies, user acceptance model.

1 Introduction

Using the Internet in a great multitude of settings, people leave various digital tracks that are being used for profiling and identification [13]. Although privacy-enhancing technologies (PETs) can help online users to protect their privacy, not many PETs found their way into the everyday life [18]. Most frequently stated reasons for the poor adoption are the difficulties for non-specialists to grasp the purpose of the technologies and the necessity of privacy protection, and also poor usability of the tools.

Privacy Attribute-Based Credentials (Privacy-ABCs) is a specific PET that allows users to minimally disclose certified information when authenticating with online service providers [5, 2–4]. In general, Privacy-ABCs are issued just like ordinary cryptographic credentials (e.g., X.509 credentials) using a digital (secret) signature key. However, Privacy-ABCs allow their holder to transform them into a new token, called *presentation token*, in such a way that the privacy of the user is protected. Still, these transformed tokens can be verified similarly to ordinary cryptographic credentials (using the public verification key of the issuer) and offer the same strong security.

T. Tryfonas and I. Askoxylakis (Eds.): HAS 2014, LNCS 8533, pp. 375–386, 2014.

Two prominent examples of Privacy-ABC systems available today are IBM's Idemix [10] and Microsoft's U-Prove [15]. The EU-funded project ABC4Trust [1] has built a unified architecture for Privacy-ABCs that abstracts away the differences between the specific implementations and ensures their interoperability. Most importantly, the project is the first to deploy Privacy-ABCs in real-life environments through pilot scenarios. This motivated us to study the problem of adoption of Privacy-ABCs by users.

Contribution. In this work, we are the first to investigate the user acceptance of Privacy-ABCs. We use the pilot deployment of Privacy-ABCs at the University of Patras, Greece to explore the experiences of users with the technology and to build a first, tentative model of user acceptance. We identify some shortcomings of the previous technology acceptance models when they are applied to PETs and present some interesting relationships between the considered user acceptance factors. For example, understanding of the Privacy-ABC technology is correlated to the perceived usefulness of Privacy-ABCs. Moreover, perceived ease of use is correlated to the intention to use the technology. This confirms the conventional wisdom that understanding and usability of technology play important roles in the user adoption of PETs.

Roadmap. This paper is organized as follows. We first discuss related work in Section 2 and then explain the concept of Privacy-ABCs and the course evaluation system in Section 3. We present our research methodology in Section 4. Descriptive statistics on the usage and acceptance of the Privacy-ABCs are discussed in Section 5. We present the resulting user acceptance model in Section 6, discuss limitations of this work in Section 7 and conclude in Section 8.

2 Related Work

User acceptance studies for security- or privacy-enhancing technologies are rare. We are only aware of two explorations that are similar to our topic, although they focus on different technologies. Spiekermann [17] investigates the consumer acceptance of PETs for RFIDs in the hypothetical scenario of RFID-based retail. Sun et al. [19] conducted a laboratory experiment and a qualitative study about user acceptance of single sign-on for websites.

Our study focuses on the adoption of Privacy-ABCs in a real scenario of course evaluation in contrast to Spiekermann's hypothetical scenario of PET usage for RFID. Thus, our users actually have experience with a Privacy-ABC prototype, which places them in a more realistic position to assess the technology. We note, however, that the demographic distribution of the participants in our study is very restricted in comparison to Spiekermann's representative sample of German population, as all our users are computer science students that participated in the ABC4Trust pilot.

Sun et al. investigate single sign-on, an existing mature security technology that is already being used for some time on the web sites, such that users have some experience with it. In comparison, Privacy-ABCs are a pilot development that is not ready for the market yet. The qualitative study by Sun et al. resulted

in a tentative user acceptance model for single sign-on. We considered this model when developing our explorative quantitative study.

User acceptance of technology has been a very active research topic in information science. Starting in late 80-ties, the Technology Acceptance Model (TAM) [7, 8] has been developed and refined for different technology types [16, 11]. We used the TAM in our study as a starting point of investigations.

Graf et al. investigate in the scope of the EU project PrimeLife [9] challenges in designing HCI for PETs. Understanding PET-related terms and the complex background mechanisms are identified as factors influencing the interaction of the users with the technology. Wästlund et al. [21, 20] study the users' mental models of the data minimization property of Privacy-ABCs. However, the adoption of Privacy-ABCs by users has not been studied so far.

3 Privacy-ABCs for the Course Evaluation

User trial performed by ABC4Trust took place at University of Patras in Greece. Privacy-ABCs were used by the university students in order to anonymously access an electronic course evaluation system at the end of the semester. The first round of the pilot was conducted during the winter term 2012, and this work is based on the data collected during that round.

3.1 Course Evaluation with Privacy-ABCs

Course evaluations have become standard practice in most universities around the world. They are usually conducted anonymously in order to ensure credible results. Privacy-ABC technology is employed in the pilot to guarantee that no identifying information about the students that submit the evaluations is sent to the system. At the same time, the Privacy-ABC system guarantees that only eligible students can have access to the evaluation of a course. That is, the system verifies that a student (1) is enrolled in the university, (2) has registered to the course and (3) has attended most of the lectures of that course.

Although the above conditions can be partly satisfied by paper-based and by other electronic course evaluation systems, it is difficult (and sometimes impossible) to ensure all of them. For example, in the paper-based evaluation, students can be de-anonymized by their handwriting. When the evaluations are conducted through computers, the students often need to put a lot of trust into the systems and into the technical staff. In both cases, ensuring that only the students that attended most of the lectures can evaluate the course requires quite a lot of effort.

To satisfy the above requirements, each student in the ABC4Trust pilot obtains a smart card that is used to receive credentials issued by the university, as shown in Fig. 1. These credentials will be used by students at the end of the semester to prove the desirable properties, i.e., to verify their enrollment in the university and their registration for the course without revealing their identity. The students utilize the same smart card to anonymously collect evidence for

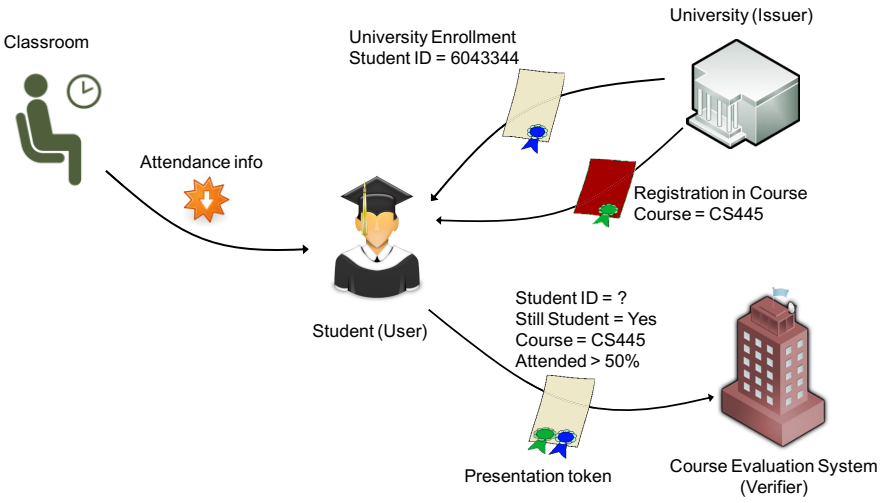

Fig. 1. The participating entities and the information flow in the Patras pilot

their class attendance throughout the semester by waving the card in front of a NFC (near field communication) device installed in the lecture room.

At the end of the semester, they *anonymously* authenticate from their PCs to the online evaluation website of the corresponding course by combining the credentials they have collected. That is, the students authenticate by proving that they are registered to the course and they have attended more than 50% of the lectures for the specific course. The technology behind the scene does not allow the card owners to exchange their obtained credentials or submit more than one evaluation for the same course. The students can make periodic backups of their smartcards such that in case of loss they can restore their credentials content to a new smartcard.

3.2 Properties of Privacy-ABCs

The ABC4Trust course evaluation system has the following properties:

- *Pseudonymity:* A student can authenticate to the system under a pseudonym. No one else (including a malicious issuer) can present a matching pseudonym to hijack the user's identity.
- *Selective Disclosure:* The students are able to prove the desirable properties, e.g. to verify their enrollment to the course, without disclosing more information.
- *Untraceability:* The evaluation system cannot connect the evaluation of two different courses back to the same student.
- *Unlinkability:* The system cannot connect a presentation token with the issuance of any of the underlying credentials.

– *Consumption Control:* The students cannot submit more than one evaluation for the same course.

4 Research Methodology

4.1 Research Questions

Our main research objective is to investigate the factors that drive user acceptance of Privacy-ABCs. Taking into account the extensions made by Pavlou [16] to the original technology acceptance model [7, 8], and also considering extensions proposed by Sun et al. [19], we identified the following factors and their relationships with each other, see also Fig. 2.

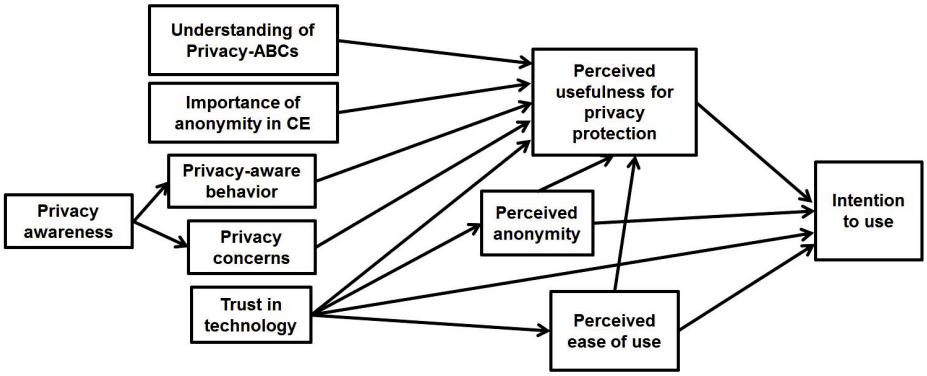

Fig. 2. Hypothetical Technology Acceptance Model for Privacy-ABCs

Perceived usefulness and perceived ease of use are the most important influencing factors on the intention to use the technology according to the original TAM. As the goal of Privacy-ABCs is to protect privacy of the users, we consider the perceived usefulness of Privacy-ABCs for privacy protection in our TAM. Pavlou [16] integrated trust into the online vendor and perceived risk of transactions into the TAM in order to investigate user acceptance of e-commerce. We also think that trust into the Privacy-ABC technology is going to positively influence perceived usefulness for privacy protection and perceived ease of use. The latter influence is justified by Pavlou with the argument that the users feel that they do not need to monitor their transactions with the system closely if they trust the system, and thus their mental effort in using the system decreases.

Instead of perceived risk that negatively influences intention to use the system, we consider perceived anonymity as a reverse construct in the context of Privacy-ABCs. The reason behind this is that the users are exposed to the risk of de-anonymization during and after the course evaluation. Thus, we assume that perceived anonymity will positively influence intention to use. Just as perceived

risk is negatively influenced by trust in Pavlou's model, we assume that perceived anonymity will be positively influenced by trust in our TAM.

Moreover, we think that understanding the privacy-protecting properties of Privacy-ABCs will positively influence perceived usefulness of Privacy-ABCs. This agrees with the observation by Sun et al. [19] that the misunderstanding of the singel sign-on technology negatively impacts adoption intentions. We also assume that the perceived usefulness for privacy protection will be positively influenced by the subjective importance of anonymity protection for course evaluations.

We also hypothesize that privacy awareness and privacy concerns will play an important role in perceived usefulness of Privacy-ABCs. We decided also to measure privacy-aware behavior (i.e., user's behavior that protects user's privacy), as we assume that privacy awareness manifests itself through privacy concerns and privacy-aware behavior.

The above influencing factors were measured either using adapted measurement scales from the literature or single questions, see section 4.3 below.

4.2 Sample and Data Collection

80 computer science students that enrolled in the course "Distributed Systems I" were given an introductory lecture on Privacy-ABCs and 48 of them decided to take part in the trial. They were given smartcards and corresponding readers, as well as supporting material (manual and videos). The printouts of the questionnaire were distributed to the pilot participants at the end of the semester. We received 41 filled out questionnaires. Thus, all further descriptions relate to the sample size of 41 subjects (28 male, 12 female, 1 not specified, 23 years old on average).

4.3 Measurement Scales

In the first data analysis step, we run an exploratory factor analysis with a Varimax rotation to ensure the one-dimensionality and hence the validity of the measured reflective constructs. Secondly, we conducted several reliability tests to assure the reliability of each measurement scale. Due to space limit we cannot present our scales here, but they are available on request from the authors.

The *perceived ease-of-use* as well as the *perceived usefulness for privacy protection* of the Privacy-ABC technology were measured with items adapted from Davis [7] on a 5-point Likert scale ranging from "strongly disagree" to "strongly agree". Whereas the adapted items of the perceived ease of use scale used almost the exact wording of the original items (for example, "I would find the Privacy-ABC system easy to use"), the perceived usefulness scale had to be adapted much more heavily, as the original scale concentrates very much on productivity, such as quickness, effectiveness and efficiency of task execution. As we measure the usefulness not for task execution but for privacy protection, we had to remove four items and to add four new ones that were adapted from Spiekermann [17]. However, during the analysis we had to drop two reverse coded items in order

to ensure validity and reliability. Both constructs are one-dimensional (KMO > 0.679, total variance explained > 51.59%) and reliable (Cronbach $\alpha > 0.676$).

The *behavioral intention to use* was assessed with the single question about the intention to use the Privacy-ABC system in future course evaluations. *Importance of anonymity in course evaluation* and *perceived anonymity* were also assessed with single questions.

To measure the *privacy concerns* of the participants we used the Westin Index [12] to classify them into privacy fundamentalist, pragmatic or unconcerned. Measured on a 5-point Likert scale the construct shows one-dimensionality (KMO = 0.539, total variance explained = 50.68%). Unfortunately, the reliability is low (Cronbach $\alpha = 0.449$).

Understanding of the concepts underlying the Privacy-ABCs was measured with six knowledge statements that refer to different aspects of the concept, such as pseudonymity, minimal disclosure or untraceability as discussed in section 3.2. For example, the statement "When I authenticate to the system, the smartcard transmits its unique serial number" was designed to test the understanding that interactions with the system are pseudonymous, that is, the system cannot identify the users (and their cards), and thus no serial number can be transmitted. The statements could be marked with "true", "false" and "don't know".

Similarly, *privacy awareness* was also measured with knowledge questions about privacy issues, for example about the usage of cookies, or about connections between IP address and user's location and personal data. To measure *privacy-aware behavior*, we asked the participants about their usage of different privacy protection mechanisms, such as cleaning cookies or browsing in private mode.

To measure *trust*, we constructed an new formative scale that asked about the trust into the different stakeholders: the developers of the system, the ABC4Trust project, the environment (University of Patras) and the underlying cryptographic algorithms.

5 Descriptive Results

Understanding of Privacy-ABCs. According to the results (see Fig. 3), most participants had difficulties with understanding of the underlying concepts, as more than 50% of them answered 4 out of 6 questions incorrectly or indicated that they do not know the right answer. The majority of the students believed that the smartcard transmits more information than it actually does, including the information that can eventually identify them, e.g. the smartcard serial number or the number of class attendances.

Perceived Ease of Use. Most participants found the system easy to use (m=3.658, σ=0.656 on a 5-points Likert scale). One aspect of the usability of the technology is the involvement of a smartcard that the users had to carry with them and where class attendance information is stored. Therefore, it is important that the

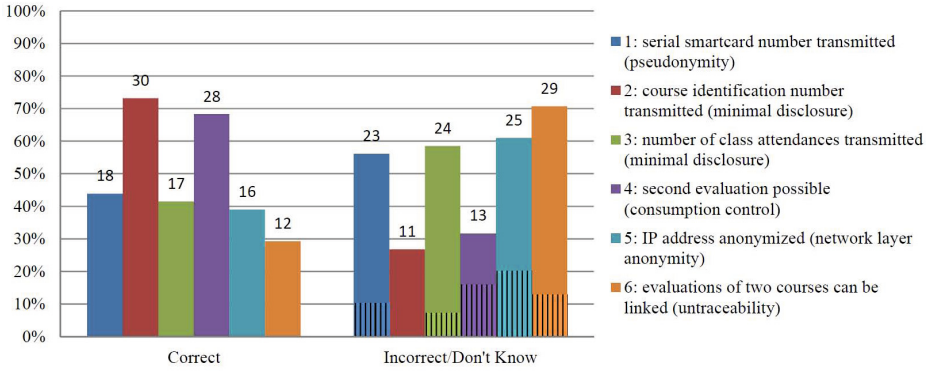

Fig. 3. Understanding of Privacy-ABCs. The left side of the graph shows the percentage of the students that answered the knowledge questions correctly. The right side shows both those who answered incorrectly or chose 'don't know'. The latter is shown by the bars filled with vertical lines.

user does not lose the smartcard. We asked the users whether they were worried that they might lose the smartcard during the semester. Most of them (68%) replied that they were not or little worried about it, while 29% appeared to be more worried. However, only 14% of the users stated that they used the backup tool for the smartcard information during the semester.

Perceived Usefulness. Most participants found the system useful for protecting their online privacy (m=3.689, σ=0.627 on a 5-point Likert scale). In addition, we explored how useful students found Privacy-ABCs in the specific scenario of course evaluation. Whereas 58.5% of the users had experience with paper-based course evaluation, only 7.3% had used an electronic course evaluation system before the trial. All students strongly agreed that protecting their anonymity in a course evaluation is important to them (mean 4.39 on a 5-point Likert scale). Comparing the paper-based evaluation with the evaluation using Privacy-ABCs, students found that using Privacy-ABCs is both more convenient and guarantees their anonymity better. Overall, 87.8% of the students declared that they would prefer a course evaluation system based on Privacy-ABCs, as opposed to 12.2% of the students that would prefer a paper-based system.

Privacy Concerns, Privacy Awareness, Privacy-aware behavior. Participants expressed a relatively high level of privacy concerns, as 34.1% were classified as privacy fundamentalist and the rest as pragmatic according to Westin Index. Privacy awareness was generally high: on average, 84.55% of the questions were answered correctly. The results of privacy-aware behavior varied a lot between different privacy protection actions. For example, while 88% of the students responded that they sometimes clean the cookies and history from their browser, only 29% of them have ever encrypted an email. 49% sometimes use the private mode in their browser, while 66% stated that they sometimes refrained

from creating a web account or making an online purchase because of privacy concerns.

Trust into the Privacy-ABC technology. The participants also had a high level of trust into the system (m=3.378, σ=0.761 on a 5-points Likert scale) that varied very marginally between the different stakeholders.

6 Tentative User Acceptance Model for Privacy-ABCs

We looked into correlations between the variables in order to build a first, tentative acceptance model for Privacy-ABCs. The resulting user acceptance model is depicted in Fig. 4 and only partly confirms the hypothetical TAM from the Fig. 2. The perceived ease of use is the most important factor in user acceptance, whereas the perceived usefulness does not directly influence the intention to use the system. Although the users have high level of trust into the system, it is not correlated to any other variables. Understanding of the technology is connected to the perceived usefulness, as expected.

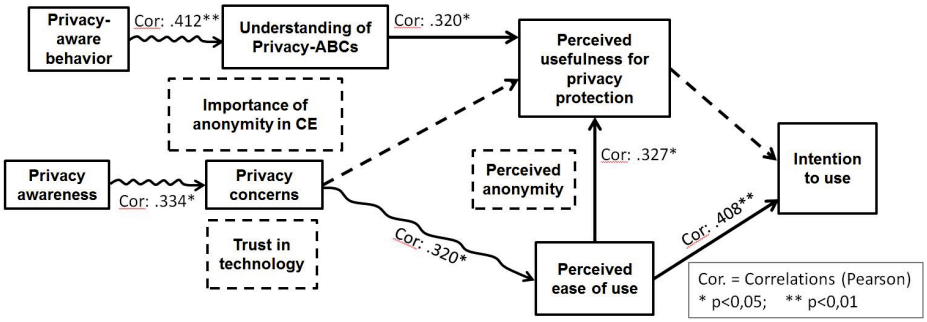

Fig. 4. Technology Acceptance Model for Privacy-ABCs resulting from the data analysis. Constructs that are not correlated to the core concepts of TAM (perceived usefulness, perceived ease of use and intention to use) are depicted in dashed rectangles. Some of the hypothetical, but not confirmed correlations are depicted with dashed lines, and some of such correlations are omitted for clarity of presentation. New (not anticipated) correlations are depicted with curly lines.

Quite surprisingly, trust is not connected to perceived usefulness and perceived ease of use. Probably another kind of trust should be measured here. We measured trust into stakeholders, but there is also a notion of trust into the specific technology as developed by McKnight et al. [14] that is probably more appropriate in our context.

Most interesting is the absence of the correlation between perceived usefulness for privacy protection and intention to use. However, security- and privacy-enhancing technologies have a property that is not characteristic for all other

technology types: it usually serves not only the primary goals of the users, but also their secondary goals [6]. Primary goal of the users in the Patras pilot is the course evaluation. However, we only measure perceived usefulness of Privacy-ABCs for the secondary goal which is the privacy protection. Considering perceived usefulness for both primary and secondary goals may favorably change the relationships between the variables in our TAM.

The correlation between privacy-aware behavior and the understanding of Privacy-ABCs is also quite interesting. It seems that people that use PETs in their everday life also better understand the ideas underlying privacy-protecting technologies.

7 Limitations

This work has several limitations that make it difficult to generalize the results. For example, all participants are computer science students, meaning that they are technically savvy and interested in technology. With other user groups, especially the results on ease of use might be quite different. Moreover, the pilot system was not actually designed with usability in mind. Better usability might have improved the understanding of system properties, as showed by Wästlund et al. [20].

8 Conclusion and Future Work

In this work, we present the first statistical results on users' understanding, usage and acceptance of attribute-based credentials, also called Privacy-ABCs. When trying to build and verify a technology acceptance model for Privacy-ABCs, we met with several difficulties that were not present in the previous TAM-related works. Especially the fact that security- and privacy-enhancing technologies usually assist both, the primary and the secondary goal of the users, was not addressed in the previous and in the presented models. On the other hand, we found some interesting relationships between the considered constructs. Thus, understanding of the Privacy-ABC technology is correlated to the perceived usefulness of Privacy-ABCs. Moreover, perceived ease of use is correlated to the intention to use the technology. We hypothesize that the strong influence of usability will even increase for users with the lower levels of privacy concerns and with less technological experience. Based on the findings from this work, we developed an improved version of the TAM for Privacy-ABCs that is going to be tested in the second run of the University of Partras pilot deployment in winter term 2014.

Acknowledgments. The research leading to these results has received funding from the European Community's Seventh Framework Programme (FP7/2007-2013) under Grant Agreement no. 257782 for the project Attribute-based Credentials for Trust (ABC4Trust) and was also supported by the Bavarian State Ministry of Education, Science and the Arts within the scope of research association ForSEC (www.bayforsec.de).

References

1. ABC4Trust: Attribute-based Credentials for Trust. EU-funded research and development project (accessed on April 26, 2013)
2. Brands, S.A.: Rethinking public key infrastructures and digital certificates: building in privacy. The MIT Press (2000)
3. Camenisch, J.L., Lysyanskaya, A.: An efficient system for non-transferable anonymous credentials with optional anonymity revocation. In: Pfitzmann, B. (ed.) EUROCRYPT 2001. LNCS, vol. 2045, pp. 93–118. Springer, Heidelberg (2001)
4. Camenisch, J., Lysyanskaya, A.: Signature schemes and anonymous credentials from bilinear maps. In: Franklin, M. (ed.) CRYPTO 2004. LNCS, vol. 3152, pp. 56–72. Springer, Heidelberg (2004)
5. Chaum, D.: Security without identification: transaction systems to make big brother obsolete. Commun. ACM 28(10) (October 1985)
6. Cranor, L.F., Garfinkel, S.: Security and Usability: Designing Secure Systems that People Can Use. O'Reilly (2008)
7. Davis, F.D.: Perceived usefulness, perceived ease of use, and user acceptance of information technology. MIS Quarterly, 319–340 (1989)
8. Davis, F.D.: User acceptance of information technology: system characteristics, user perceptions and behavioral impacts. International Journal of Man-Machine Studies 38(3), 475–487 (1993)
9. Graf, C., Wolkerstorfer, P., Hochleitner, C., Wästlund, E., Tscheligi, M.: HCI for PrimeLife Prototypes. In: Camenisch, J., Fischer-Hübner, S., Rannenberg, K. (eds.) Privacy and Identity Management for Life, ch. 11, pp. 221–232. Springer (2011)
10. IBM Research Zurich. Idemix, `http://www.zurich.ibm.com/security/idemix`
11. King, W.R., He, J.: A meta-analysis of the technology acceptance model. Information & Management 43(6), 740–755 (2006)
12. Kumaraguru, P., Cranor, L.F.: Privacy indexes: A survey of Westin's studies. Institute for Software Research. Paper 856 (2005)
13. Mayer, J., Mitchell, J.: Third-party web tracking: Policy and technology. In: 2012 IEEE Symposium on Security and Privacy, SP (2012)
14. Mcknight, D.H., Carter, M., Thatcher, J.B., Clay, P.F.: Trust in a specific technology: An investigation of its components and measures. ACM Transactions on Management Information Systems (TMIS) 2(2), 12 (2011)
15. Microsoft Research. U-Prove, `http://research.microsoft.com/en-us/projects/u-prove`
16. Pavlou, P.A.: Consumer acceptance of electronic commerce: integrating trust and risk with the technology acceptance model. International Journal of Electronic Commerce 7(3), 101–134 (2003)
17. Spiekermann, S.: Privacy enhancing technologies for RFID in retail- an empirical investigation. In: Krumm, J., Abowd, G.D., Seneviratne, A., Strang, T. (eds.) UbiComp 2007. LNCS, vol. 4717, pp. 56–72. Springer, Heidelberg (2007)
18. Spiekermann, S., Cranor, L.: Engineering privacy. IEEE Transactions on Software Engineering 35(1) (2009)
19. 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)

20. 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)
21. Wästlund, E., Fischer-Hübner, S.: The users' mental models' effect on their comprehension of anonymous credentials. In: Camenisch, J., Fischer-Hübner, S., Rannenberg, K. (eds.) Privacy and Identity Management for Life, ch. 12, pp. 233–244. Springer (2011)