The Effect of Semantic Elaboration on the Perceived Security and Privacy Risk of Privacy-ABCs - An Empirical Experiment

Ahmad Sabouri

The Effect of Semantic Elaboration on the Perceived Security and Privacy Risk of Privacy-ABCs — An Empirical Experiment

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. Privacy-ABCs are elegant techniques to deliver secure yet privacy-enhanced authentication solutions. The cryptography behind them enables new capabilities, such as selective disclosure of attributes, set membership, and predicates over attributes, which many of them were never experienced by typical users before. Even if the users intuitively accept the existence of such features, they may not be still ready to perceive the semantic of such a proof within the context of authentication. In this work, we argue that additional information is necessary to support the user understand the semantic of their operations. We present the results of our empirical experiment on investigating the effect of providing such a support during authentication with Privacy-ABCs on the perceived security and privacy risk of the users.

1 Introduction

The research community has been trying to enhance the strong authentication techniques to respect the privacy of the users. More specifically, efforts have been dedicated to design schemes for providing data minimization, unlinkability and untraceability during an authentication session. In this regard, *Privacy-preserving Attribute-based Credentials (Privacy-ABCs)*, also known as anonymous credentials, have been in the focus of various recent research projects such as Prime, PrimeLife, FutureID, and ABC4Trust. From the different flavours of Privacy-ABCs, the IBM Idemix and Microsoft U-Prove are among the most prominent ones. Privacy-ABCs are cryptographically proven to be unlinkable and untraceable. Thus, the service providers cannot tell whether two tokens were generated by the same user or not. Also the issuers cannot trace tokens back to the issuance phase and the person behind them, unless the disclosed attributes contains some identifying information.

Privacy-ABCs come with new capabilities such as *selective disclosure of attributes*, *predicate over attributes*, and *proof of set membership*, which mainly were never experienced by the users in any of the previous authentication schemes. For instance, using *predicates over attributes*, a user is able to prove facts such as

less than or *greater than* about their attributes without actually disclosing the attribute value itself. Taking the example of our experiment, a service provider can request a "German" user to prove if her postal code is in the range of 59999 to 61000. In this way, the service provider learns that the user is living in the city of Frankfurt am Main but it does not learn in which district of the city, which could possibly cause leak of information about the financial status. Some scholars [8] reported that users lack an appropriate mental model for such technologies regarding even simpler features, such as combining individual attributes from different credentials in a single authentication. Consequently, we argue in this paper that without additional support regarding the semantic of their actions, the users may not be appropriately influenced by such privacy-enhancing technology regarding their security and privacy risk perception.

In this paper, we demonstrate that the users' perception of security and privacy risks changes, when they are supported with additional information regarding the semantic of their proofs during authentication with Privacy-ABCs. Our findings are based on the results of an empirical experiment with 80 users. We compared the perceived security and privacy risk of two groups of participants who received different treatments during their practice of authentication with Privacy-ABCs. For this experiment, we first implemented an experiment platform where the user could practice authentication with Privacy-ABCs. In the next step, we used the platform to conduct the experiment with the users and afterwards measured their perceived security and privacy risk using part of a systematically developed measurement instrument (cf. Appendix A).

In the rest of this paper, we review the previously conducted related research in Section 2. Later on, we explain the details of our experiment in Section 3. The results and implications of our experiment are provided in Section 4. In the end, we conclude the paper in Section 5.

2 Related Works

To the best of our knowledge, there have not been many studies in the literature concerning the human aspects of Privacy-ABCs. Wästlund et. al. [8] were the first ones who reported about the challenges to design user-friendly interfaces that convey the privacy benefits of Privacy-ABCs to users. They observed that users were still unfamiliar with the new and rather complex concept of Privacy-ABCs, since no obvious real-world analogies existed that could help them create the correct mental models. Benenson et al. [2, 3] investigated one of the ABC4Trust trials using the Technology Acceptance Model (TAM) [4]. Benenson et. al. discovered significant negative correlation of Perceived Risk with the Intention to Use, the Perceived Usefulness for the first and secondary goals, the Perceived Ease of Use and the Trust. In the same study, they found the Perceived Risk to be dependent to Perceived Anonymity.

An experts survey was conducted in [7] to predict the factors influencing adoption of Privacy-ABCs. The results indicate that the complexity for the user is among the most important factors. In our study, we try to reduce the complex-

Items	Concept Behind
I think by using ID+ to login to Politiks.eu, my various posts at Politiks.eu become linkable together.	Linkability
I believe by using ID+ to login to Politis.eu, I will be able to use the Politiks.eu anonymously/pseudonymously.	Anonymity
I think Politiks.eu is not secure enough to be used with ID+.	Security
I believe using ID+ to login to Politiks.eu puts other services, which are used with ID+, at risk and enables unauthorised/unwanted actions at those other services.	Unwanted Authorization
I believe using ID+ to login to Politiks.eu leads to identity theft or impersonation.	Impersonation
I believe that my usage of ID+ to login to Politiks.eu leads to loss of privacy for me because my personal data are collected without my knowledge and consent.	Collection
I believe by using ID+ to login to Politiks.eu, I lose control over my personal data.	Control
I believe by using ID+ to login to Politiks.eu, my posts at Politiks.eu become known to the ID+ operator.	Traceability

Table 1. Measurement Instrument for Security and Privacy Risk of using ID+ to Authenticate towards Politiks.EU

ity by providing additional support for the semantic analysis of the *presentation policies* (which are the artefact describing the requested attributes and proofs by service providers) and observe the effect on the perceived security and privacy risks, because perceived risk is reported to be particularly important for the adoption of e-services [6]. The method to influence the perceived risk was chosen based on the recommendations of the warning theory. The warning theory suggests that more specific information about hazards and consequences can reduce uncertainty and enable people to make better-informed cost-benefit trade-off decisions regarding the need to comply [5]. Bal [1] extended this design theory to the field of information privacy warning design by experimentally investigating the effects of explicitness in privacy warnings on individuals' perceived risk and trustworthiness of smartphone apps and observed significant effects.

3 Experiment Design

The experiment was designed to evaluate the effect of additional semantic analysis of the *presentation policy* on the perceived privacy risk by end users. We first implemented the necessary software components to enable authentication with Privacy-ABCs. We called our mock-up Privacy-ABC identity card as "ID+" and let the users try it in our experiment portal, "Politiks.eu". We also adjusted our developed questionnaire for the perceived security and privacy risk to reflect our experiment environment (the details of developing the questionnaire are presented in Appendix A). We used a 7-points Likert scale in the questionnaire ranging from *Strongly disagree* to *Strongly agree*. Table 1 demonstrates the final questionnaire for our experiment. Then, we conducted the experiment through the network of the students at the Goethe University Frankfurt in October and November 2015. In the following sections, we explain the details of our process.

3.1 Experiment Platform Setup

A precondition for our experiment was to set up a platform where scenarios for authenticating with Privacy-ABCs could be tried out. We decided to develop a mock-up prototype which presents the workflow of authenticating with

1. Open Firefox
2. Plug your smart card into the reader
3. Check your data on the card
4. What information about your is stored on the ID+ smart card?
5. Close the ID+ window
6. Question: *How can you check your data again if you want?*
7. Open "http://politiks.eu"
8. *The portal is introduced!*
9. Login to the "Frankfurt Mayor" discussion
10. Follow the authentication steps
11. What is happening now?
12. Question: *What is the website going to learn about you?*
13. Have a look at the posts
14. Write a post and send it
15. Check your post
16. Log out
17. Login to the "Drug" discussion
18. Follow the authentication steps
19. Question: *What is the website going to learn about you?*
20. Have a look at the posts
21. Write a post and send it.
22. Check your post
23. Log out
24. Login to the "Mayor" discussion again
25. Follow the authentication steps
26. Have a look at your previous posts
27. Write a new post and send it
28. Check your post
29. Log out.

Fig. 1. User Tasks List

Privacy-ABCs with a more friendly interface than the ABC4Trust reference implementation and better integration into the web browser. We designed the User Agent as a Firefox plugin and integrate it into the browser.We added a button, called "ID" into the toolbar of the Firefox browser, which upon clicking, it would show the users' identity credential in case the smartcard was connected to the computer. In the experiment, the authentication was emulated, therefore, the smart card was employed to provide the feeling of a real process but the users' attributes were actually stored in the browser configurations. A small Java application was developed to run in the background in order to check the status of the smartcard, which allowed the browser plugin to query the status via a Restful web-service call. The plugin was designed to attach specific Javascript codes to the html content of the web-page when opening the experiment portal URL. The Javascript codes would provide the possibility of communicating with the plugin in order to invoke the GUI for authentication with Privacy-ABCs. When a button on the web-page triggers login with Privacy-ABCs, the message is communicated to the plugin. The GUI would pop up as small window next to the "ID" button if the smart card is present. The window guides the user through the steps of authentication and upon completion the user is redirected to the requested page.

3.2 Conducting the Experiment

The experiment was conducted within the student community of the Goethe university Frankfurt. The only limitation was to limit the age to be between 18 and 34. The participants were randomly assigned to one of the two envisioned groups, the "control group" and the the "experiment group". All participants received a brief introduction of ID+ and its privacy-enhancing features. Afterwards, the participants were given a smartcard and were asked to open Firefox and browse to the experiment portal, "http://politiks.eu". In order to urge the

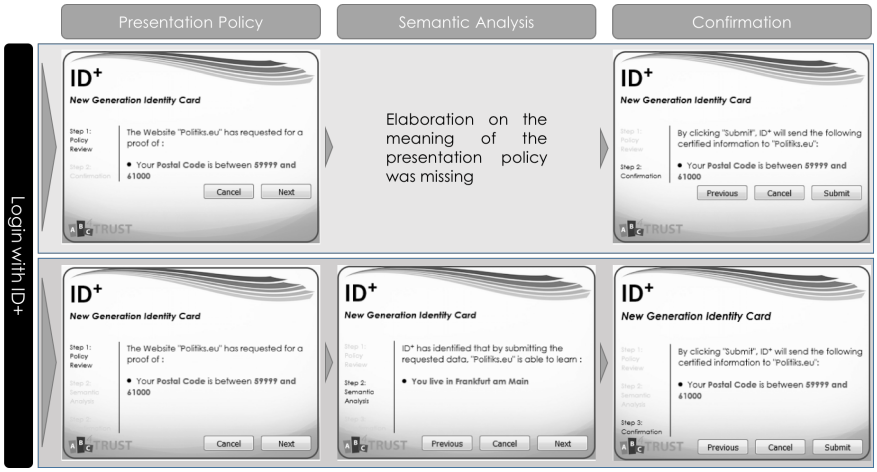

Fig. 2. Experiment Process

need for privacy, we decided the deliver political discussion as the main content of the portal. Two forums were initiated in the portal; one about mayoral election in the city of Frankfurt and one about legalizing drugs. Each forum required the user to authenticate with her ID+ in order to get access to the discussion. The process of authenticating with ID+ for the two groups are shown in Figure 2. Upon clicking on "Login with ID+" the respective GUI would pop up to guide the participant through the authentication process. The Frankfurt mayoral election forum asked the users to deliver a proof for "Your Postal code is between 59999 and 61000" and the forum on legalizing drugs, would request the users a proof of "Your birth date is before the 01.01.1997". The former policy semantically means that the participant is living in the Frankfurt am Main area as the postal code is following 60xxx format, and therefore the forum ensures that she is a stakeholder. The latter also proves that the participant is older than 18 (by the time of the experiment) and consequently allowed to discuss about drugs. A semantic analysis of the given access policy was presented to the participants of the "experiment group" and not to the "control group". This additional step was the only difference of the process between the two groups and it was introduced as an additional transparency mechanism which could influence the perceived privacy risk of the users. The participants were guided through a task list (presented in Figure 1) to interact with the portal. In the end, each participant was asked to fill the questionnaire that we developed to measure their perceived security and privacy risk with regard to the use of ID+.

4 Results and Implications

In total 80 participants took part in the experiment, 35 female and 45 males. All the participant were between 18 and 34 years old. Regarding the education

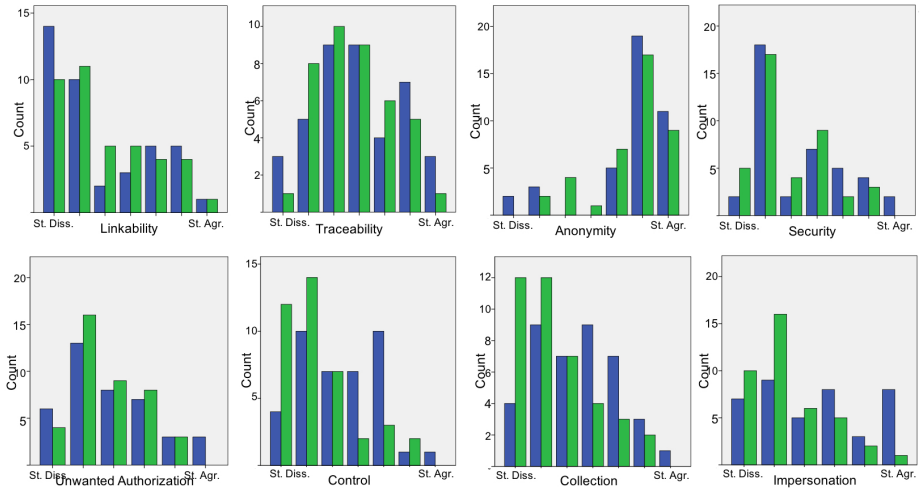

Fig. 3. Participants' Answers to the Security and Privacy Risk Questions. First Column = Control Group, Second Column = Experiment Group

level, 13 had no university degree yet, 42 hold a Bachelor's degree, and 25 had Master's degree or above. We statistically analysed the questionnaire results using the IBM SPSS tool. Perceived security and privacy risk is a complex construct and can have various factors. Within the items measuring the perceived security and privacy risk, we covered various aspects namely, Linkability, Traceability, Anonymity, Security, Control, Collection, Impersonation and Unwanted Authorization.

The responses to each of the questions are demonstrated in Figure 3. The x-axis represents the answers (1 = Strongly Disagree, 2 = Disagree, 3 = Somewhat Disagree, 4 = Neither Agree nor Disagree, 5 = Somewhat Agree, 6 = Agree, 7 = Strongly Agree).

Comparing the descriptive statistical values for the answers of the control group and the experiment group, we can say both groups *Somewhat Disagreed* to the risk of Linkability ($m_c = 2.85, \sigma_c = 1.96, m_e = 2.95, \sigma_e = 1.78$). With regard to Traceability, both groups had on average a neutral perception ($m_c = 3.98, \sigma_c = 1.72, m_e = 3.75, \sigma_e = 1.46$. The results concerning Anonymity were almost the same for both groups and laid between *Somewhat Agree* and *Agree* ($m_c = 5.60, \sigma_c = 1.67, m_e = 5.50, \sigma_e = 1.41$). For Security, the experiment group demonstrated a slightly stronger disagreement compared to the control group but in general they were both around *Somewhat Disagree* ($m_c = 3.38, \sigma_c = 1.72, m_e = 2.88, \sigma_e = 1.44$). The results also indicate a slight difference concerning perception of Unwanted Authorization but the average on both groups was close to *Somewhat Disagree* ($m_c = 2.93, \sigma_c = 1.46, m_e = 2.75, \sigma_e = 1.13$). The perception of the control group was on average between *Somewhat Disagree* and *Neutral* towards Impersonation while the experiment group's perception was be-

	Component	
	C1	C2
Unlinkability	.150	.736
Anonymity (rev)	.101	.830
Impersonation	.701	.208
Collection	.894	.052
Control	.887	.177
Untraceability	.464	.470
Unwanted Authorization	.467	.448
Security	.603	.358

Table 2. Rotated Component Matrix. Rotation Method Varimax with Kaiser Normalization.

	Leven's Test for Equality of Variance		t-test for Equality of Means						
	F	Sig.	t	df	Sig. (2-tailed)	Mean Diff.	Std. Error Diff.	95% Confidence Interval of the Diff	
								Lower	Upper
C1 Equal variances assumed	3.809	.055	2.887	78	.005	.72500	.25108	.22513	1.22487
Equal variances not assumed			2.887	73.092	.005	.72500	.25108	.22460	1.22540
C2 Equal variances assumed	3.396	.069	.030	78	.976	.00833	.27932	-.54774	.56441
Equal variances not assumed			.030	71.051	.976	.00833	.27932	-.54860	.56527

Table 3. Independent Samples T-test

tween *Disagree* and *Somewhat Disagree* ($m_c = 3.38, \sigma_c = 1.78, m_e = 2.40, \sigma_e = 1.28$). A similar result was observed for Collection ($m_c = 3.48, \sigma_c = 1.57, m_e = 2.50, \sigma_e = 1.47$), and Control ($m_c = 3.40, \sigma_c = 1.53, m_e = 2.40, \sigma_e = 1.43$).

We performed a *Principal Component Analysis (PCA)* using Varimax rotation with Kaiser Normalization on the security and privacy risk items to investigate whether all the items were loading one "total security and privacy risk" or not. To perform a PCA, the rule of thumb is to have at least 10 participants per variable, which our total number of participants met this requirements for our eight variables. As shown in Table 2, the results indicate that our eight items were loading two components (which we named C1 and C2). Consequently, we calculated component C1 as an un-weighted average of Security, Unwanted Authorization, Impersonation, Collection and Control, and also C2 as the unweighted average of Unlinkability, Untraceability and Anonymity. Regarding the reliability test, the Bartlett test indicated significant correlation and the Kaiser-Meyer-Olkin (KMO) measure verified the sampling adequacy for the analysis with KMO = .789. Moreover the Cronbach's α was calculated as 0.82 and 0.6 for C1 and C2, respectively.

After identifying the components, we compared the mean value of C1 and C2 between the control group and the experiment group using a *Independent Samples T-test*. As reported in Table 3, the results demonstrate statistically significant difference of C1 between the two groups, p-value $\leqslant 0.005$, which means that the probability of the corresponding difference in the means to occur by chance is less than or equal to 0.5%. This shows that the participants of the experiment group perceived less risk (mean diff. = .725) concerning the

dimensions of security and privacy covered by C1. Intuitively, the experiment group received additional explicit information with regard to the consequences of delivering the proofs requested by the portal, which made them specially perceive better control over their attributes and their collections.

5 Conclusion

In this work, we designed and conducted an empirical experiment with Privacy-ABCs in order to demonstrate the effect of additional supports to the users with regard to the semantic of the Privacy-ABC proofs. Privacy-ABCs enable new privacy features such as minimal disclosure, predicate over attributes, and set membership. However, users are not very familiar with those concepts and have difficulties to build a mental model of such advanced operations. We argued that additional information explaining the facts and semantics of required Privacy-ABC proofs during an authentication process has an influence on the perceived security and privacy risk of the users. We verified our hypothesis through our experiment, where we examined 80 participants in two groups and measured their perceived security and privacy risk using our systematically developed measurement instrument. Our results demonstrated that the group who received additional information about the semantic of the proofs had a statistically significant difference in some aspects of their perceived security and privacy risk. Despite following methodological approaches, the experiment was conducted through the student network of the Goethe University Frankfurt and the age of the participants were limited to 18-34 years old. Consequently, the results may not be generalizable to users who are significantly different from our sample group.

References

1. Bal, G.: Explicitness of consequence information in privacy warnings: Experimentally investigating the effects on perceived risk, trust, and privacy information quality. In: Proceedings of ICIS 2014, Auckland, New Zealand, Dec. 14-17 (2014)
2. Benenson, Z., et. al.: User acceptance of privacy-abcs: An exploratory study. In: HCI (24). pp. 375–386. Springer (2014)
3. Benenson, Z., et. al.: User acceptance factors for anonymous credentials: An empirical investigation. In: Proceedings of WEIS (2015)
4. Davis, F.D.: Perceived usefulness, perceived ease of use, and user acceptance of information technology. MIS quarterly pp. 319–340 (1989)
5. Laughery, K.R., Wogalter, M.S.: Designing effective warnings. Reviews of human factors and ergonomics 2(1), 241–271 (2006)
6. 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)
7. Sabouri, A.: Understanding the determinants of privacy-abc technologies adoption by service providers. In: Proceedings of I3E 2015, Delft, The Netherlands, October 13-15, 2015. pp. 119–132 (2015)
8. Wästlund, E., et. al.: Evoking comprehensive mental models of anonymous credentials. In: Open problems in network security, pp. 1–14. Springer (2012)

A Appendix: Developing a Measurement Instrument

Designing an appropriate and robust measurement instrument is an essential part of any experiment. One of the contributions of this paper is the systematic development of an instrument which measures *multi-faceted risk* of using an identity management solution to access a service. Perceived risk is theorized as being multi-dimensional [3]. Jacoby and Kaplan [5] defined the following five components of risk: financial, performance, physical, psychological, social, and the overall risk. Roselius [10] also identified a sixth dimension called Time loss. Featherman and Pavlou [4] proposed to consider privacy risk in the context of e-commerce instead of the physical risk which seems to be very unlikely. Since then multi-faceted risk has been considered in various studies such as adoption of Internet Banking [6], initial acceptance of emerging technologies [7], and self-service technologies and e-services [3]. Table 4 introduces the dimensions we considered in our instrument.

Dimension	Definition
Performance Risk	User assessment of potential performance problems and malfunctioning, transaction processing errors, etc., and therefore not delivering the service as promised.
Financial Risk	User assessment of potential financial losses due to the employment of an Identity Service Provider XXX and its login mechanism for accessing Service Provider YYY.
Security & Privacy Risk	User assessment of potential security violation or losses to the privacy and confidentiality of their online/offline identity, personal data, or activities
Time Risk	User assessment of potential losses to convenience, time and effort caused by wasting time researching, setting up, switching and learning how to use the Identity Service Provider XXX login process.
Psychological Risk	User assessment of potential losses to their self-esteem, peace of mind or self-perception (ego) due to worrying, feeling frustrated, foolish, or stressful as a result of employing an Identity Service Provider XXX to login to the Service Provider YYY
Social Risk	User assessment of potential losses to their perceived status in their social group as a result of using and Identity Service Provider XXX to access the Service Provider YYY. The assessment of the probability that consumers believe that they will look foolish to important others
Physical Risk	User assessment of potential losses to their health and their physical status

Table 4. Facets of Risk for the use of Identity Management Systems

In this work, we followed the three stages proposed by Moore and Benbasat [8] in order to develop an instrument to measure the multi-faceted risk of using an identity management solution to authenticate towards a service. The first stage aims at the identification of existing items and the creation of new ones which fit to the definition of the respective constructs.

The second stage focuses on assessing the construct validity and refining ambiguous items. This stage was done following the approach by Anderson and Gerbing [2] by a pretest assessment of the substantive validities of the measures, which is achieved by an *item-sorting task*. In this iterative exercise, some representatives of the population were asked to judge each item and assign it to the construct to which they think the item belongs. After carrying out each round,

two indices were calculated: *proportion of substantive agreement*, P_{sa}, and *substantive validity coefficient*, Csv. The indices range from 0.0 to 1.0 and from -1.0 to 1.0 respectively.

P_{sa} is defined as the proportion of respondents who assign an item to its intended construct. The equation for this calculation is: $P_{sa} = nc/N$ where nc represents the number of people assigning an item to its posited construct and N represents the total number of respondents. Csv represents the extent to which respondents assign an item to its posited construct more than to any other construct. The formula for this index is: $C_{sv} = (nc - no)/N$, where nc and N are defined as before and no indicates the highest number of assignments of the item to any other construct.

Larger values for both indices show greater substantive validity and the recommended threshold is 0.5. We conducted the pretest with the help of 20 participants. Even though the majority of the constructs met the threshold, we had to do some refinements in order to improve the items and remove ambiguity. The second round was performed by involving 7 participants, which verified the validity of all the constructs. Table 5 represents the results of the tests.

	Round 1			Round 2		
Construct	Items	P_{sa}	C_{sv}	Items	P_{sa}	C_{sv}
Performance Risk	3	0.84	0.78	3	0.90	0.86
Financial Risk	3	0.90	0.80	3	1.00	1.00
Security & Privacy Risk	8	0.83	0.77	8	1.00	1.00
Time Risk	2	0.92	0.85	2	0.86	0.71
Psychological Risk	2	0.55	0.28	2	1.00	1.00
Social Risk	2	0.93	0.88	2	0.93	0.86
Physical Risk	3	0.96	0.93	3	1.00	1.00

Table 5. caption here

The final version of the multi-faceted risk measurement instrument is as follows:

Performance:

- Identity Service Provider XXX does not perform reliable enough to guarantee access to Service Provider YYY at anytime. (adapted from [3])
- Identity Service Provider XXX goes down (unreachable) and therefore creates problem with my access to Service Provider YYY. (adapted from [3])
- In future Identity Service Provider XXX discontinues its service and incurs trouble for me to access Service Provider. (new based on the identified risks by [1])

Financial:

- Using Identity Service Provider XXX to login to Service Provider YYY leads to financial loss for me. (adapted from [3])

- Using Identity Service Provider XXX to login to Service Provider YYY stands me to lose money. (adapted from [4])
- Using Identity Service Provider XXX to login to Service Provider YYY causes undesired/unintended withdrawal from my financial (e.g. bank) accounts. (adapted from [4])

Security and Privacy:

- If I use Identity Service Provider XXX to login to Service Provider YYY, my various transactions/service usages at Service Provider YYY become linkable together. (new based on terminology by [9])
- Using Identity Service Provider XXX to login to Service Provider YYY, I will be able to use the service anonymously/pseudonymously. (new based on terminology by [9])
- Service Provider YYY is not secure enough to be linked to Identity Service Provider XXX. (new)
- Using Identity Service Provider XXX to login to Service Provider YYY puts other service providers, which are linked to Identity Service Provider XXX, at risk and enables unauthorized/unwanted actions at those other services. (new due to widespread use of OAuth)
- Using Identity Service Provider XXX to login to Service Provider YYY leads to identity theft or impersonation. (new based on the identified risks by [1])
- My usage of Identity Service Provider XXX to login to Service Provider YYY leads to loss of privacy for me because my personal data are collected without my knowledge and consent. (adapted from [4])
- Using Identity Service Provider XXX to login to Service Provider YYY, I lose control over my personal data. (adapted from [3])
- Using Identity Service Provider XXX to login to Service Provider YYY, my usage of Service Provider YYY becomes known to Identity Service Provider XXX. (new based on terminology by [9])

Time:

- I have to waste a lot of time if I need to switch from Identity Service Provider XXX to another one in the future for accessing Service Provider YYY. ((adapted from [3])
- I have to spend lots of time on setting up and learning how to use Identity Service Provider XXX to login to Service Provider YYY. (new)

Psychological:

- Using Identity Service Provider XXX to login to Service Provider YYY makes me nervous or anxious. (new)
- Using Identity Service Provider XXX to login to Service Provider YYY makes me feel worried. (adapted from [3])

Social:

- Using Identity Service Provider XXX to login to Service Provider YYY harms the way others think of me. (adapted from [3])
- Using Identity Service Provider XXX to login to Service Provider YYY leads to a loss of status and reputation for me because my friends and relatives will think less highly of me. (adapted from [3])

Physical:

- Logging into Service Provider YYY using Identity Service Provider XXX is not safe; i. e. may be (or become) harmful or injurious to my health. (adapted from [5])
- Using Identity Service Provider XXX to login to Service Provider YYY leads to physical harm by governmental organizations. (new)
- I will get physically hurt by others if I login to Service Provider YYY using Identity Service Provider XXX. (new)

References

1. Ackermann, T., Widjaja, T., Benlian, A., Buxmann, P.: Perceived it security risks of cloud computing: conceptualization and scale development (2012)
2. Anderson, J.C., Gerbing, D.W., Hunter, J.E.: On the assessment of unidimensional measurement: Internal and external consistency, and overall consistency criteria. Journal of marketing research pp. 432–437 (1987)
3. Featherman, M.S., Hajli, N.: Self-service technologies and e-services risks in social commerce era. Journal of Business Ethics pp. 1–19 (2015)
4. Featherman, M.S., Pavlou, P.A.: Predicting e-services adoption: a perceived risk facets perspective. International journal of human-computer studies 59(4), 451–474 (2003)
5. Jacoby, J., Kaplan, L.B.: The components of perceived risk. Advances in consumer research 3(3), 382–383 (1972)
6. Lee, M.C.: Factors influencing the adoption of internet banking: An integration of tam and tpb with perceived risk and perceived benefit. Electronic Commerce Research and Applications 8(3), 130–141 (2009)
7. Luo, X., Li, H., Zhang, J., Shim, J.: Examining multi-dimensional trust and multi-faceted risk in initial acceptance of emerging technologies: An empirical study of mobile banking services. Decision support systems 49(2), 222–234 (2010)
8. 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)
9. Pfitzmann, A., Hansen, M.: A terminology for talking about privacy by data minimization: Anonymity, unlinkability, undetectability, unobservability, pseudonymity, and identity management (2010)
10. Roselius, T.: Consumer rankings of risk reduction methods. The journal of marketing pp. 56–61 (1971)