Simply tell me how—On Trustworthiness and Technology Acceptance of Attribute-Based Credentials

Rachel Crowder
Newcastle University
Newcastle upon Tyne, United Kingdom

George Price
Newcastle University
Newcastle upon Tyne, United Kingdom

Thomas Groß
Newcastle University
Newcastle upon Tyne, United Kingdom

ABSTRACT

Attribute-Based Credential Systems (ACS) have been long proposed as privacy-preserving means of authentication, yet have not found wide-spread adoption to date. We ask what factors explain whether users will adopt ACS or not. To that end, we aim to comprehend how factors interrelate to predict ACS technology acceptance and to investigate how intrinsic and presentation aspects of the ACS cause the intent to use them. We conducted two between-subject, random-controlled trials with a combined UK-representative sample of $N = 812$ participants. After having stated their privacy concerns and faith-in-technology, each participant then inspected one variant of an ACS website, which encoded a combination of three intrinsic aspects and three presentation aspects of an ACS. Participants then reported on the perceived trustworthiness, perceived usefulness, and their behavioral intention to adopt the technology. We proposed an extended Technology Acceptance Model incorporating privacy concern and perceived trustworthiness and show in covariance-based structural equation modeling that the model explains user decision making very well. We could show that communicating facilitating conditions and demonstrating results drives the overall technology acceptance. Communicating with simple language impacted the behavioral intent to use the ACS positively. Our work is the first to show cause-effect relations for ACS adoption with substantial sample size. This study not only informs what factors impact the technology acceptance of ACS, but likely also translates to other privacy-enhancing technologies and yields methodological considerations for research into the privacy paradox at large.

KEYWORDS

attribute-based credential systems, perceived trustworthiness, technology acceptance

1 INTRODUCTION

Attribute-Based Credential Systems (ACS) and anonymous credential systems specifically promise to protect the users' privacy in a wide range of scenarios. They have been implemented by industry behemoths such as IBM and Microsoft with Identity Mixer and U-Prove, respectively. They found some adoption in, for instance, the IRMA Card [23, 59] of Radboud University or the the collaboration between Microsoft Research and Signal, headed for deployment in the Signal client [16]. However, in the big scheme of things ACS failed to reach broad adoption.

The technical and socio-economic challenges and the herculean task of building a sustainable ACS eco system notwithstanding, it remains an open question whether users would widely adopt ACS granted their availability. Furthermore, it is an open question what human aspects of ACS implementation and presentation would consistently drive such an adoption.

Earlier studies indicated that Technology Acceptance Model (TAM) [57] could be a decent framework to investigate the users' behavior in ACS. An empirical correlational analysis by Benenson et al. [4] with $N = 30$ university students from Patras supported technology adoption modeling in this fashion, albeit with limited analysis capabilities and at low statistical power. Similarly, recent work by Harborth and Pape [34] showed that a TAM-inspired partial least squares path model with $N = 141$ users could fit the adoption of the mix-network JonDoNym quite well. While this result is not on ACS themselves, its model is instructive vis-à-vis of the aforementioned analysis of Benenson et al. Overall, the works of Harborth and Pape [34, 35] could explain roughly $R^2 \approx 42\%$ of the variance of the user's behavioral intention to use the PETs. Can we do better than that?

As the given models were focused on modest extensions of core TAM, they did not incorporate important factors such as facilitating conditions for perceived trustworthiness or results demonstrability for technology acceptance. Hence, these earlier works could suffer from missing factors indicated as a concern in the privacy paradox literature [37]. In addition, prior studies did not offer experimental manipulations to establish cause-effect relations what steps could boost adoption. Hence, to date we lacked a robust and comprehensive model for the perceived trustworthiness and technology acceptance of Attribute-Based Credential Systems.

Aims. We ask the research question what factors influence the technology acceptance of ACS. We investigate which intrinsic properties of an ACS could benefit adoption, that is, which aspects of an ACS, e.g., the provider, the users take into account for trustworthiness and adoption. We further consider which presentation properties of its delivery channel will impact perceived trustworthiness and technology acceptance. For example, to what extent does it make a difference when the properties of the ACS are expressed in simple language versus in technical jargon.

Our Contributions. (i) We establish the first large-scale study with $N = 812$ participants representative of the UK population to establish a robust SEM of perceived trustworthiness and technology acceptance of Attribute-Based Credential Systems. Compared to earlier works, our study competes on breadth and depth in establishing

Proceedings on Privacy Enhancing Technologies 2024(4), 544–564

https://doi.org/10.56553/popets-2024-0129

an extended technology acceptance model, which explains twice the variance of the users' behavioral intention to adopt the system compared to earlier studies on ACS and PETs in general. Our work, thereby, yields the best ACS technology acceptance model available to date. (ii) Our study creates the first model for PETs technology acceptance including facilitating conditions and results demonstrability as antecedents. While these factors have been investigated in extended technology acceptance models [57, 58], we are the first to show that they make a difference for PETs. (iii) We are able to show a partial mediation by perceived usefulness concerning the impact of privacy concerns on behavioral intention. Both earlier kinds of studies of Benenson et al. [4] and Harborth and Pape [34] did not provide conclusive evidence on that front. (iv) This study is the first to establish a random controlled trial with systematic manipulation of causes influencing perceived trustworthiness and technology adoption in a between-subjects design. Unlike earlier works, this approach enables us to quantify how design decisions such as the use of layman language causes increased adoption. (v) Our results are not only instructive for the technology-acceptance decision making of users on ACS and similar privacy-enhancing technologies, they also offer methodological considerations for the privacy paradox at large.

2 BACKGROUND

This work investigates human factors involved in the adoption Attribute-Based Credential Systems (ACS) primarily using the Technology Acceptance Model (TAM) and measures of perceived trustworthiness as foundations. We introduce these topics in turn.

2.1 Attribute-Based Credential Systems

Originally conceptualized by David Chaum [17] in the form of anonymous credential schemes, Attribute-Based Credential Systems (ACS) bear the promise of authentication without identification and, thereby, form an essential privacy-enhancing technology. One strand of development starting from Brands' construction [9] became the ACS Microsoft U-Prove. Another based on one of the first breakthrough constructions by Camenisch and Lysyanskaya [13] was developed into the IBM Identity Mixer ACS [15]. The latter was subsequently extended with methods for revocation [12], efficient attribute encoding [11], and smart card enablement [6], all technical advancements towards the adoption in government-certified identity cards and passports. Later advancements were made in elliptic-curve instantiations [14, 55].

More recent advancements include the development of the IRMA Card [23, 59], a smart card version of ACS with selective disclosure as well as the ACS deployment for Signal to achieve privacy-preserving authentication of Signal groups [16]. Furthermore, ACS were expanded to graph signature [29] and relational anonymous credential schemes [56], for which the model in this paper likely also holds.

2.2 Model Foundations

2.2.1 Technology Acceptance Model. The *Technology Acceptance Model* (TAM) was first developed by Davis [21, 22] as an adaptation of the Theory of Reasoned Action. TAM is one of the most widely adapted frameworks to explain computer usage behavior. Davis [21] founded the content validity of the model on three bodies of research: (i) the impact of perceived usefulness on system utilization, (ii) the impact of perceived ease of use on self-efficacy, and (iii) the cost-benefit paradigm from behavioral decision theory. The model itself was developed in a step-by-step process to develop scales for perceived usefulness and perceived ease of use, which were refined and confirmed in successive factor analysis. The model has undergone a considerable history of scrutiny [40, 44, 54].

Subsequently, Venkatesh and Davis extended the technology acceptance model with a range of antecedents such as subjective norms and results demonstrability in TAM 2.0 [57]. The content validity of the added constructs stems from the theory of rational action and the theory of planned behavior. Venkatesh and Davis also determined that subjective norms can influence intention indirectly through internalization and identification. While Pavlou [47] extended TAM 2.0 with constructs for trust and risk, Venkatesh et al. [58] further extended the model to the Extended Unified Theory of Acceptance and Use of Technology (UTAUT2), which was, in turn, used as a foundation for perceived trustworthiness scales reused in the field. TAM and its variants are supported by longstanding research and have been extended to model user behavior in privacy-enhancing technologies, such as Attribute-Based Credential Systems [4] and Mix-Networks [34].

Given the different variants of TAM, we considered the following antecedents: From TAM 2.0 [57], we included faith in technology and privacy concerns in the place of subjective norms. We did not include image, job relevance, and output quality as they are not relevant for ACS. Result demonstrability, however, seemed highly relevant in measuring the user's understanding of ACS. We included it. With respect to Pavlou's extensions to TAM 2.0 [47], we incorporated perceived trustworthiness instead of a combination of trust and risk, because of a substantive body of literature on measuring this factor. In this, our work is more aligned with Harborth and Pape's [34, 35] studies of PETs than with Beneson et al. [4]. From the antecedents of UTAUT2 [58], we perceived facilitating conditions as most relevant for ACS, modeling aspects highlighted in PETs qualitative studies [33, 50]. Hedonistic motivation, price value and habit are not relevant for the scenario of downloading a new ACS. We anticipated that social influence would only come into play once ACS were more well-known. We omitted UTAUT2 moderation variables in the SEM, that is, experience, voluntariness, age, and gender.

2.2.2 Measuring Perceived Trustworthiness. The Cambridge Dictionary defined trustworthiness as "the quality or fact of being able to be trusted." We investigated a range of options to measure perceived trustworthiness, especially with the context of online and computer systems. The investigated instruments are sourced predominately from the areas of marketing and e-commerce. In our investigation, we found a distinction between a perceived trustworthiness of a provider and the perceived trustworthiness of a system or artifact.

In terms of Perceived Provider Trustworthiness, Lee and Turban [39] focused on trust in online merchants, distinguishing between merchant properties, medium properties and contextual properties. Gefen [27] considered different dimensions of trust and trustworthiness for electronic commerce. Büttner and Göritz [10]

discussed measures of trust for online shops. The latter scale includes ability, benevolence, integrity, and predictability, the former three having been used by Lee and Turban and Gefen, as well.

For Perceived System Trustworthiness on the other hand, Corritore et al. [19] investigated the perceived trustworthiness of websites, and considered as constructs honesty and reputation and risk. Bart et al. [3] evaluated website trustworthiness including as antecedents of trust factors such as privacy, security, and absence of errors.

In a separate line of work, McKnight et al. [45] investigated trust in specific technologies, including general faith in technology and trusting stance, which we adopted to measure covariates.

Alalwan et al. [1] extended the technology acceptance model with notions of trust, which used a trust scale by Gefen. Due to the affinity to the Technology Acceptance Model, we chose this scale as the measurement of perceived trustworthiness.

2.2.3 Measuring Privacy Concern. There exist a range of instruments measuring privacy concern, well documented for instance by Preibusch [48]. For this study, we chose Internet Users Information Privacy Concern (IUIPC) [43] as the privacy concern instrument. This choice is aligned with Harborth and Pape's choice of the scale in the investigation of the adoption of Tor [35]. Information privacy concern is defined as "an individual's subjective views of fairness within the context of information privacy." IUIPC is heavily influenced by the earlier scale Concern for information privacy (CFIP) [52], which focuses on organizational privacy. IUIPC has received scrutiny in terms of its validity and reliability [30]. While the instrument was reported to show good pedigree in terms of content validity, there were weaknesses found wrt. the reliability of the sub-scales control and awareness, which led to the proposal of an eight-item brief scale called IUIPC-8 [31].

2.3 The Privacy Paradox

The privacy paradox, that is, the dichotomy between privacy attitudes and privacy behavior has been researched extensively in the field. Dienlin and Trepte [24] studied the privacy paradox in online social network scenarios distinguishing between informational privacy, social privacy and psychological privacy. They modeled a SEM relating privacy concerns, privacy attitude, privacy intention and privacy behavior. They observed a partial mediation of the impact of privacy attitude on behavior through privacy intention and concluded that the privacy paradox was largely present. On the other end of the spectrum, Solove [53] reflected on the privacy paradox considering behavior valuation and behavior distortion arguments and arguing that the privacy paradox does not exist. A systematic literature review by Gerber et al. [28] extracted standardized effect sizes from a wide range of publications in the field to quantify observed effects that could explain the privacy paradox. This study, however, did not quantify these effects in a nomological network. Kokolakis [37] reviewed explanations including the users' conceptualizations of privacy and their privacy calculus, heuristics, biases and bounded rationality. Unlike Gerber et al. [28], Kokolakis also named methodological issues including inappropriate/incomplete models, missing factors, and inappropriate research methods. Subsequent research [30] added validity and reliability of privacy concern scales and the expected attenuation their impact on behavioral factors to the methodological concerns. Our study will explore such considerations, as well.

2.4 Structural Equation Modelling

We will employ *covariance-based structural equation modeling* with a reflective measurement model. In a *reflective measurement model*, the indicators are *endogenous*, that is, caused by the latent factors. Kline [36] offers an excellent introduction to the methodology. Anderson and Gerling [2] discuss the multi-step modeling approach we will employ. In terms of human factors in privacy research, Groß [31] considers validity and reliability challenges for privacy concern scales and corresponding models relevant for this work.

Modelling non-normal, ordinal data as in the models introduced in Section 2.2 requires special attention. Standard maximum likelihood (ML) estimation assumes the multivariate normality for the joint population distribution of the endogenous variables, given the exogenous variables [36]. This can only hold for continuous variables. Hence, analyzing ordinal data such as obtained from Likert scales from self-report instruments introduced above with ML estimation may yield inaccurate results [25]. The structural equation model community has discussed a range of appropriate alternatives [8]. To make the point, Liddell and Kruschke [41] illustrated misrepresentations that can occur when ordinal data is analyzed in metric models.

To establish accurate models on non-normal, ordinal data, we turn to diagonally weighted least square estimation with robust standard errors and a mean- and variance adjusted test statistic (WLSMV). In general, WLSMV models are more complex to comprehend, because they operate on a probit-estimation and thresholds for choosing a level of an indicator. They also require a greater sample size than ML models. Furthermore, Shi et al. [51] cautioned that the RMSEA fit index could be inaccurate especially for larger models with more than $p = 20$ covariance observations. They advocated SRMR as a fit estimate that stays accurate especially with a larger sample size ($N \geq 500$). We will take these considerations into account in our model evaluation.

Mediation analysis [42] refers to the analysis of variable arrangements for a main relation $X \rightarrow y$, in which changes in a third variable Z, the mediator, are both caused by independent variable X and cause changes in the dependent variable Y. Commonly, mediation is tested with the *causal-steps approach*, which requires that, given significant relations, the absolute coefficient between X and Y must be larger in a model excluding the mediator paths than in a model including the mediator paths. We distinguish *complete* and *partial* mediation, based on the coefficient between X and Y is still statistically significant, adjusted for the mediation through Z. In an *inconsistent* mediation at least one mediated effect has a different sign than other mediated or direct effects in a model [42]. For ordinal data, mediation is best analyzed on standardized coefficients.

3 RELATED WORKS

Perceived Trustworthiness & Technology Acceptance of ACS. Benenson et al. [4] investigated the perceived trustworthiness and technology acceptance of ACS after a preliminary examination of the subject [5]. They issued ACS smart cards to distributed systems students of Patras University and received $N = 30$ observations

from their questionnaires. While the use of smart cards offered the study greater ecological validity, it suffers in terms of sample quality and statistical power. In terms of research design, Benenson et al. [4] specified a new TAM model and offered the reliability statistics for the new instruments. They distinguished primary and secondary task in keeping with the observation in usable security that those are processed differently. We follow their lead in this design choice.

Benenson et al. included risk and trust in their instruments, similar to Pavlou's extension of TAM [47], however only used a single item for these two constructs. We perceived single-item constructs fraught with statistical perils (being ordinal and non-normal, unreliable, not yielding an identified construct for a latent factor) and, thereby, opted for well-vetted comprehensive scales on perceived trustworthiness. The Patras study did not model privacy concern. Instead, it included perceived anonymity, situational awareness, and importance of anonymity, but did not include the latter in its final model. We chose to follow the TAM 2.0 [57] conceptualization more closely and included privacy concern and faith in technology in place of subjective norms.

Benenson et al. concluded that "the sample size (30 participants) is prohibitively small for deeper statistical analysis such as multiple regressions or structural equation modeling;" we agree to this cautious assessment. Indeed, based on the small sample the study made 45 pair-wise Kendall correlation tests with FDR multiple-comparison corrections at overall low statistical power. In contrast, our study is the first to evaluate technology acceptance of anonymous credentials based on a large nationally representative sample and to offer the statistical power for the deeper analysis and structural equation modeling missing in this prior work.

Trustworthiness and Technology Acceptance of PETS. Harborth and Pape [34] established a partial least square structural equation model (PLS-SEM) with SmartPLS on a sample of JonDonym[1] users. JonDonym is not an ACS, but a mix-net service which was founded on the Java Anon Proxy. Their study focuses especially on the role of perceived anonymity and trust. $R^2 = 42.9\%$ of the variance of behavioral intention are explained by its antecedents. The work contrasted with the aforementioned work of Benenson et al. [4] in that it found strong effect of trust on the behavioral intention to use the PET. Harborth and Pape established a structural equation on $N = 141$ questionnaire responses from anonymous users. Following the guidance by Hair et al. [32], we note that PLS path modeling focuses on maximizing the variance explained and on theory development. The competing covariance-based SEM (CB-SEM) is more appropriate for confirmatory research. Even though PLS-SEM has been frequently criticized in the field, a number of researchers came eloquently to its defense [32]. PLS-SEM is generally non-parametric and robust in face of distribution problems. It can cope with smaller sample sizes than CB-SEM, everything else being equal.

In subsequent work, Harborth and Pape [35] investigated technology adoption considering privacy concerns, trust and risk using the a case study of Tor. Their survey study on $N = 124$ users of the anonymizer Tor using PLS-SEM underpinned that trust in Tor is a statistically significant effect on actual use. The study used IUIPC as privacy concern instrument and OPLIS as privacy literacy instrument. Instead of usefulness and ease of use investigated in TAM studies, Harborth and Pape evaluated trusting and risk beliefs as antecedents of behavioral intention, explaining $R^2 = 41.2\%$ of the variance.

We incorporated perceived trustworthiness instead of Harborth and Pape's trusting and risk beliefs as two constructs. While their study was focused of actual users of PETs and included a scale measuring how often they use the PETs in their daily life, we measured the user's download attempt as a single binary indicator, which we did not include in the final SEM due to modeling constraints. Compared to Harborth and Pape's studies, our SEM explains approximately double the variance of users' behavioral intention to adopt the PETs.

Qualitative Evaluation of User Acceptance. Harbach et al. [33] conducted a focus-group study on acceptance of privacy-enhancing authentication systems, based on a sample of 18 university students. The study evaluated the user attitudes to the German eID card nPA and highlighted issues along the lines of motivation, complexity, control, comfort, insufficient information, and cost. This qualitative work mirrors considerations we investigate quantitatively in terms of ease of use (=comfort), facilitating conditions (=complexity and control), results demonstrability (=insufficient information).

Sabouri [50] established an open-coding qualitative study of user acceptance of attribute-based credentials, based on interviews of 40 students. The study established salient benefits of ACS with selective disclosure, anonymity/pseudonymity, and transparency. Identified barriers included lack of information, lack of trust, adoption inertia, additional hardware, compromised smart-cards, and cost. Again, a range of outlined barriers correspond to factors we test in this study: results demonstrability (=lack of information), perceived trustworthiness (=lack of trust, compromised smart-cards), facilitating conditions (=adoption inertia and additional hardware).

Adoption by Service Providers. Technology adoption is not only an important factor for the users' decision making but also for service providers. Sabouri [49] first considered this question by as determinants of technology adoption by service providers. The conceptual model included (i) perceived benefits/costs, (ii) organization, (iii) environment, (iv) external pressure, and (v) technology. The corresponding empirical survey was conducted at the 2015 ABC4Trust summit based on 20 responses from the 80 expert participants and yielded a ranked list of factors. Subsequently, Krontiris et al. [38] integrated views on user adoption of attribute-based credentials based of Benenson's experiment [4] discussed above with views on service provider adoption.

4 AIMS

4.1 ACS Trustworthiness & Acceptance

Our first line of inquiry is: "*Why are users choosing to adopt ACS? What factors impact technology adoption?*" Hence, we aim at establishing a sound model of ACS trustworthiness and technology acceptance.

RQ 1 (ACS Trustworthiness & Acceptance). *We aim at establishing and confirming a robust structural latent variable model of the perceived trustworthiness and technology acceptance of ACS.*

[1] https://anonymous-proxy-servers.net

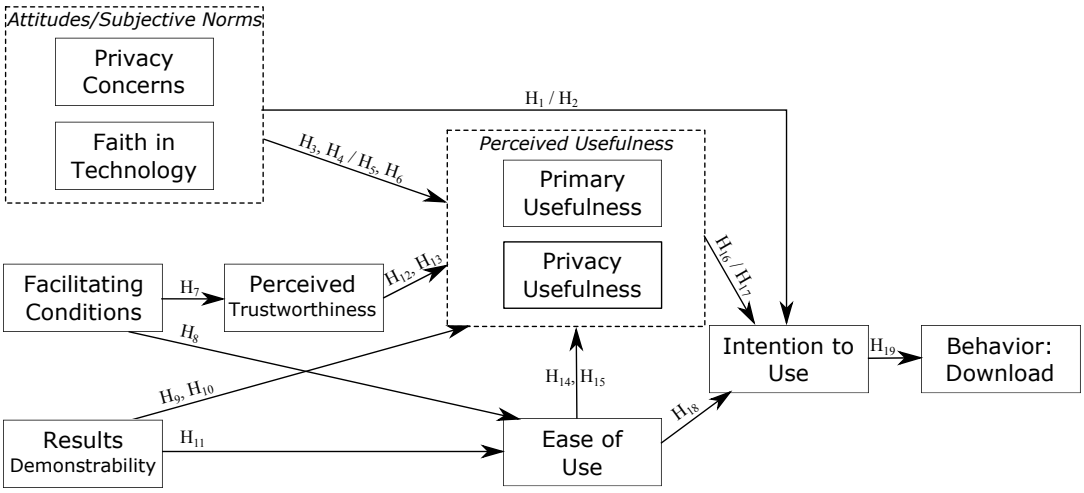


Figure 1: Nomological network of perceived trustworthiness, usefulness and technology acceptance of ACS.
Note: slash denotes different antecedents; comma denotes different consequences.

We aim at a creating structural equation model with theoretical foundations in the Technology Acceptance Model (TAM 2.0) [57] and the empirical research by Benenson et al. [4]. Figure 1 illustrates the overall planned structure. The corresponding hypotheses are yielded by the underlying theory.

Hypotheses. For brevity, we only name the alternative hypotheses and have it understood that the corresponding null hypotheses can be derived canonically.

H_1: Privacy Concerns yield a positive impact on the Intention to Use an ACS.
H_2: Faith in Technology yields a positive impact on the Intention to Use an ACS.
H_3, H_4: Privacy Concerns have a positive impact on Primary Usefulness and Privacy Usefulness, respectively.
H_5, H_6: Faith in Technology has a positive impact on Primary Usefulness and Privacy Usefulness, respectively.
H_7: Facilitating Conditions impact Perceived Trustworthiness positively.
H_8: Facilitating Conditions impact Ease of Use positively.
H_9, H_{10}: Results Demonstrability has a positive impact on Primary Usefulness and Privacy Usefulness, respectively.
H_{11}: Results Demonstrability impacts Ease of Use positively.
H_{12}, H_{13}: Perceived Trustworthiness has a positive impact on Primary Usefulness and Privacy Usefulness, respectively.
H_{14}, H_{15}: Ease of Use has a positive impact on Primary Usefulness and Privacy Usefulness, respectively.
H_{16} / H_{17}: Primary Usefulness as well as Privacy Usefulness yield a positive impact on Intention to Use.
H_{18}: Ease of Use impacts the Intention to Use positively.
H_{19}: The Intention to Use impacts the Behavior to download positively.

We call the relations between Usefulness, Ease of Use, Intention to Use, governed by Hypotheses H_{14}–H_{18}, the *Core Technology Acceptance Model.*

4.2 Impact of ACS Properties

Our second line of inquiry is the cause-effect impact of intrinsic and presentation properties of an ACS on its perceived trustworthiness and technology acceptance.

RQ 2 (Impact of ACS Properties). *We investigate to what extent*
(i) intrinsic properties of a scheme and its provider, as well as
(ii) the overall presentation and perception of the offering
impact the perceived trustworthiness, overall technology acceptance and behavioral intention to follow through with an installation.

The corresponding hypotheses model true cause-effect relations established by experimental manipulations.

Hypotheses. Again, we only name the alternative hypotheses, the prefix *C* indicating a cause-and-effect hypothesis. All hypotheses operate on the perceived trustworthiness and the antecedents of the core technology acceptance model. Note that, therefore, each hypothesis is a compound hypothesis yielding multiple statistical hypotheses operating on low-level variables.

Intrinsic Properties.

$H_{C,1}$: The provider of an ACS impacts its perceived trustworthiness and acceptance.
$H_{C,2}$: The benefits of an ACS yield an impact in that user benefits have a more positively effect than privacy benefits.
$H_{C,3}$: The usage of an ACS makes a difference in that everyday use has a more positively effect that tech usage.

Presentation Properties.

$H_{C,4}$: Simplicity of the textual content has a positive impact on perceived trustworthiness and acceptance.
$H_{C,5}$: The presence of people has a positive impact on perceived trustworthiness and acceptance.
$H_{C,6}$: The available support makes a difference on perceived trustworthiness and acceptance in that more support options yield a more positive outcome.

4.3 Mediation Analysis

Figure 1 sets up a mediation analysis of the impact of privacy concerns being mediated by perceived usefulness. In the body of the paper, we focus on a complete mediation, that is, a mediation in which only the indirect path through perceived usefulness (H_3, H_4) is modelled and the direct path (H_1) set to zero. We include a comparison of complete and partial mediation in Appendix C.

5 METHOD

This work was pre-registered in the Open Science Framework[2]. The structural equation model presented in this paper was registered as secondary analysis. The main analysis with MANOVA and OLS linear regression was conducted and reported in other outputs. For reproducibility, results, graphs and tables were computed from the datasets with the R package knitr. All test statistics are evaluated at a significance level of $\alpha = .05$. Statistical inferences are designed to be two-tailed and multiple-comparison corrected.

We hosted two experiments as part of this study, one on intrinsic properties, the other on presentation properties. The two experiments were created as a fractional factorial design, that is, each experiment is a factorial design of its own manipulations, and uses the default levels of the variables of its sister experiment as fixed values. The experiment on presentation properties of Attribute-Based Credential Systems set the provider to none. We controlled for similarity between experiments on relevant factors, such as readability.

5.1 Ethics

The studies followed the ethical guidelines of the institution and received ethical approval.

Participants entered the study under informed consent and could leave the survey at any point. Participants had the opportunity to contact the principal investigator to ask further questions. Participants were paid at slightly higher rate than required by Prolific Academic for the expected completion time of the questionnaire: £4. Participants could only enter the any constituent experiment of the study once.

To reduce bias and offer blinding, we employed deception keeping participants unaware of the true purpose of the study and of the manipulations involved. The post-survey debriefing page explained the true intentions to the participants.

5.2 Sample and Assignment

Sampling Process. We set the target population as residents of the United Kingdom. As survey population, we chose the UK residents registered on the platform Prolific Academic, the sampling frame consisting of the corresponding user list as of August 2019. Both experiments were independently sampled, with participants registered for one experiment being excluded from the other, thereby maintaining independence of observations. The sampling was conducted with a representative distribution by age, gender and ethnicity, with replacement in the case of participants not completing the full survey. Overall, the sampling process was a judgment sampling, in which participants matching the age/gender/ethnicity constraints self-selected to participate.

Sample Size. The sample size was determined with an *a priori* power analysis for covariance-based structural equation modeling: we determined an overall target sample size of 840 participants.

Concealed Random Assignment. Both experiments were designed as random-controlled trials. In both experiments, we used a simple random assignment to allocate participants to their conditions. The randomness was generated with a Javascript pseudo-random number generator.

During an experiment run, we used concealed assignment to blind the experimenters as well as the participants. We segregated the experimental environments by conditions such that participants were not aware of the interventions, that is, offering a separate survey as well as a separate Web page embedding the corresponding interventions for each condition. While experimenters were able to see the assigned conditions in the final dataset, the statistical analysis was done in covariance analysis unaware of the condition assignments.

5.3 Operationalization

We aim at measuring the factors of the technology acceptance model and participant attitudes that likely impact their behavior. To that end, we measured the participants' privacy concerns (IUIPC-10) [43], faith in technology (FIT) [45], system trustworthiness (ST) [45] and technology acceptance [57] with their corresponding factors, yielding measurement variables outlined in Table 1. While Appendix D encloses the corresponding materials, Appendix A details the operationalization itself.

In addition to measuring the antecedents of technology acceptance and perceived trustworthiness, we introduced experimental conditions that manipulated how the ACS was displayed to the participants. Here, we distinguished *intrinsic properties*, that is, how the ACS is made, and *presentation properties*, that is, how the ACS is presented to users. For each combination of these properties as an experimental condition, we constructed a Web-site variant as exemplified in Figure 2. Appendix A.2 details how the manipulations are operationalized.

To summarize, intrinsic properties include (i) who provides the ACS (provider), (ii) what benefits an ACS enables (benefits), (iii) how a user would use an ACS (usage). Presentation properties include (i) how complex a languages is used (simplicity), (ii) whether people are associated with the ACS (people), (iii) what level of tech support is available (support). A Web site variant presented to a participant realizes a combination of these properties. We consider the case that the ACS is made by a nationally known university, offers general privacy benefits and describes processes of the technology as reference condition of intrinsic properties. We define a presentation in complex language, without association with people and with no support options on the Web site as reference condition.

5.4 Procedure

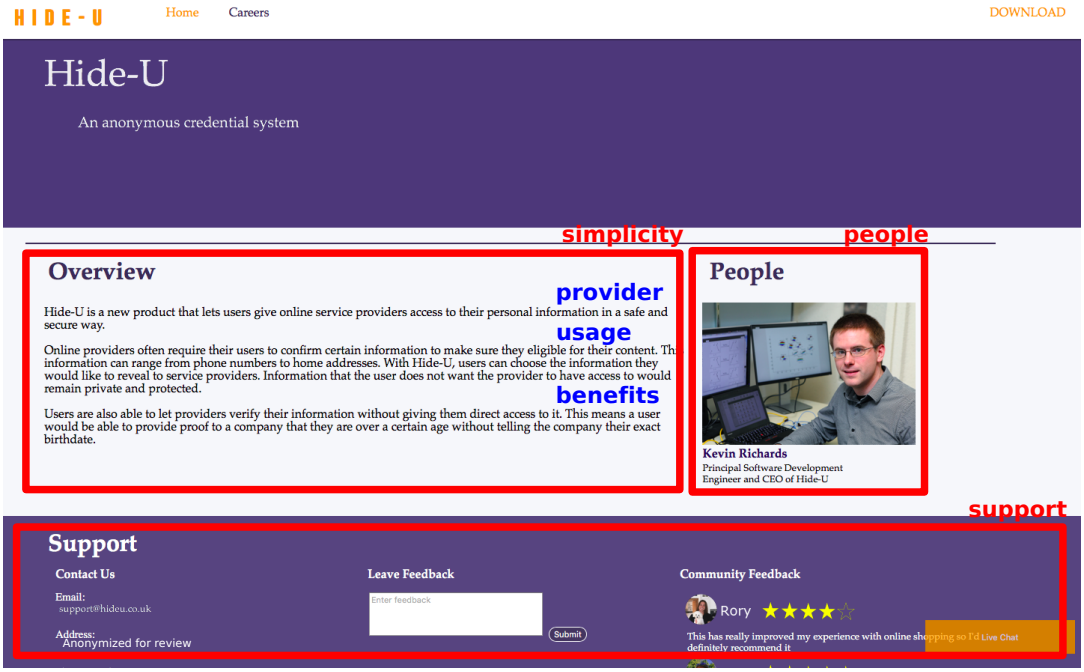
As overall procedure, participants were asked to visit a Web site on Attribute-Based Credential Systems and evaluate their properties.

[2] https://osf.io/5jd8a/

Table 1: Final operationalization of measurement variables (MVs)

	Instrument	Sub-Scale	Variable	Items
Privacy concerns	IUIPC-10 [43]	Control	ctrl	ctrl1, ctrl2, ctrl3,
		Awareness	aware	awa1, awa2, awa3
		Collection	collect	coll1, coll2, coll3, coll4
Faith in Technology	McKnight [45]	Faith	fit	MKF1, MKF2, MKF3, MKF4
		Trusting Stance	ts	MKTS1, MKTS2, MKTS3
System Trustworthiness (ST) [45]		Facilitating Conditions	fc	STFC1, STFC2, STFC3, STFC4
		Perceived Trustworthiness	trust	STT1, STT2, STT3, STT4, STT5, STT6
Technology Acceptance Model [57]	TAM 2.0	Results Demonstrability	results	TAR1, TAR2, TAR3, ~~rTAR4~~
		Primary Usefulness	primuse	STPE1, STPE2, STPE3, STPE4
		Privacy Usefulness	privuse	TAU1, TAU2, TAU3, TAU4,
		Ease of Use	ease	TAE1, TAE2, TAE3, TAE4
		Behavioral Intention (TS)	bi	STBI1, STBI2, ~~STBI3~~, STBI4

Note: rVAR = reverse-coded variable VAR; ~~VAR~~ = variable VAR removed after reliability analysis.



Note: Intrinsic variables are depicted in **blue**; presentation variables in **red**. The example site displays the condition: provider=none, usage=everyday, benefits=user, simplicity=simple, people=photo, support=fullsupport of the presentation study.

Figure 2: Overview of the interventions placed on the ACS Web site.

The condition, that is, the combination of realizations of manipulated independent variables, was embedded in the Web site the participants were directed to. Figure 3 illustrates this procedure in a nutshell. The participants proceeded as follows:

(1) First, the participants filled in questionnaires their demographics and on trait-like co-variates, such as IUIPC and general Faith and Trust in Technology.
(2) Second, participants were directed to a web site and asked to spend 10 minutes to read the Web site and form an opinion on the described Attribute-Based Credential System (ACS).
(3) Third, the participants were asked factual questions on the Web site appearance to check that they indeed completed the task.
(4) Fourth, the participants answered questionnaires on their impressions of the system, incl. on reliability, system trustworthiness, and technology acceptance, as well as their behavioral intention to use such a system.
(5) Throughout the questionnaire, the participants answered instructional manipulation checks (attention checks).
(6) Finally, in the debriefing, the participants reported how much they felt different aspects of the Web site contributed to their

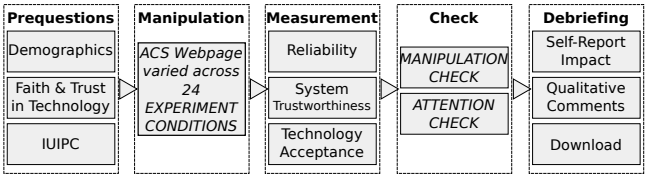


Figure 3: Overview of the experimental procedure.

Table 2: Sample Refinement

Phase	Intrinsic		Presentation		Total
	Excluded	Size	Excluded	Size	
Starting Sample		473		467	940
Incomplete	58	415	34	433	848
Duplicate	25	390	0	433	823
FailedAC> 1	36	379	0	433	812
Final Sample					812

decisions, were offered an opportunity to give qualitative comments and reconfirm their download action with a code.

We diligently established structural equation models for the covariances exhibited by the participants by paying attention to the following considerations: (i) We built the models step-by-step [2], starting from the measurement model, introducing a regression path model, and finally constructing the causal path model incorporating the experimental conditions. Through this approach, we gained confidence that each successive model constituted a better fit. (ii) We employed Weighted Least Square estimation (WLSMV) to account for the ordinal, non-normal nature of the data and to render the models robust against Type I and II errors [8]. We detail the SEM modeling methodology in Appendix B.

6 RESULTS

6.1 Sample

The initial sample consisted of 940 participants, 473 from the experiment on intrinsic properties, 467 from the experiment on presentation properties. Cases were removed from the sample without replacement based on two criteria: (i) The participant did not complete the full survey; (ii) The participant failed more than one attention check, as pre-registered. Table 2 shows the refinement to the final sample with a final $N = 812$. We provide its demographic characteristics in Table 3.

6.2 Step-by-Step Modeling

We established the final model in a step-by-step fashion, by first establishing a confirmatory factor analysis of the measurement model and then adding regression equations for the path models. In each step, we checked whether the new model offers a statistically significantly better fit with a likelihood-ratio test. We offer a comparison of the scaled fit measures of the WLSMV estimations in Table 4. We discuss intricacies of model selection and mediation effects in Appendix C.

Table 3: Demographics of the final sample

	Overall
N	812
Gender (%)	
Male	391 (48.2)
Female	414 (51.0)
Rather not say	7 (0.9)
Age (%)	
18-24	133 (16.4)
25-34	215 (26.5)
35-44	167 (20.6)
45-54	115 (14.2)
55-64	141 (17.4)
65+	41 (5.0)

6.2.1 Step 1: Measurement Model. The confirmatory factor analysis (CFA) of the measurement model includes the indicator variables and the corresponding latent variables. Hence, the CFA only includes variables specified in operationalization Table 1. The measurement model yielded a good global fit highlighted in the Measurement row of Table 4. We inspected the residuals for local fit and were satisfied. While we anticipated correlated residuals based on observations on the questionnaire, we chose not to include those in the model after the fact.

Table 5 summarizes the factor loadings of the measurement model. All loadings are estimated with high confidence and a p-value of $p < .001$. In terms of reliability, the factors ctrl and aware suffered from the lowest internal consistency, with $\omega = 0.73$ and a signal-to-noise ratio ($S/N_\omega \leq 2.76$). Privacy usefulness (privuse yields the greatest internal consistency, with $\omega = 0.95$). Overall, we assess that the measurement model is valid and sufficiently reliable to continue our investigation with the regression path model.

6.2.2 Step 2: Regression Path Model. The regression path model incorporates the measurement model established in Section 6.2.1 and adds regression equations modeling the hypothesized relations introduced in Section 4. This more complex model yielded a statistically significant improvement over the measurement model, $\chi^2(23) = 430.138, p < .001$. We evaluate the global fit of the regression path model in the Regression row of Table 4. While the scaled RMSEA of 0.07 indicates presence of residuals, the SRMR of 0.06 shows decent fit.

6.2.3 Step 3: Causal Path Model. We show the global fit of the WLSMV-estimated causal path model Causal row of Table 4. The causal model exhibits an excellent fit, evident being supported by the close-fit hypothesis, $p_{\epsilon_0 \leq .05} = .310$. We select this model as our final model.

6.3 Final Model

We include the final model this section.

6.3.1 ACS Trustworthiness & Acceptance. We report selected regression coefficients in Table 6 and discuss their consequences in the following paragraphs. Let us first consider the structural

Table 4: Scaled fit measures of the three modelling steps

Model	χ^2	df	p_{χ^2}	CFI	TFI	RMSEA	LL	UL	p_{rmsea}	SRMR
Measurement	3501.88	879.00	< .001	0.97	0.97	0.06	0.06	0.06	< .001	0.05
Regression	4122.85	902.00	< .001	0.96	0.96	0.07	0.06	0.07	< .001	0.06
Causal (final)	4064.92	1324.00	< .001	0.97	0.98	0.05	0.05	0.05	.310	0.06

Table 5: Factor loadings of the WLSMV-estimated CFA of the measurement model

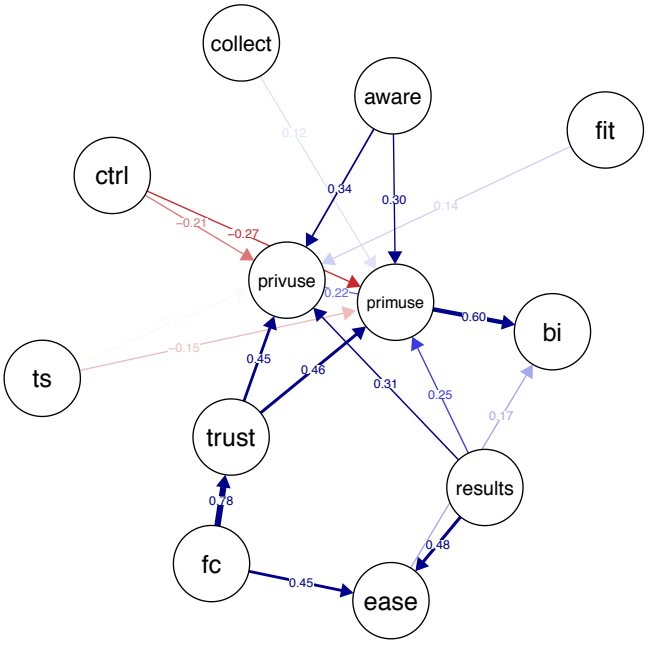
Factor	Indicator	Factor Loading				Standardized Solution				Reliability				
		λ	SE_λ	Z_λ	p_λ	β	SE_β	Z_β	p_β	R^2	AVE	α	ω	S/N_ω
fit	MKF1	1.00$^+$				0.81	0.02	35.05	< .001	0.66	0.63	0.83	0.82	4.63
	MKF2	1.02	0.04	24.43	< .001	0.83	0.02	37.90	< .001	0.68				
	MKF3	0.97	0.04	21.94	< .001	0.78	0.02	32.12	< .001	0.61				
	MKF4	0.92	0.04	20.52	< .001	0.75	0.03	26.67	< .001	0.56				
ts	MKTS1	1.00$^+$				0.90	0.01	73.09	< .001	0.82	0.78	0.87	0.90	8.67
	MKTS2	1.06	0.03	40.70	< .001	0.96	0.01	78.95	< .001	0.93				
	MKTS3	0.84	0.02	39.08	< .001	0.76	0.02	42.75	< .001	0.58				
ctrl	ctrl1	1.00$^+$				0.79	0.03	30.02	< .001	0.62	0.54	0.65	0.73	2.76
	ctrl2	0.99	0.06	17.85	< .001	0.78	0.03	30.46	< .001	0.61				
	ctrl3	0.81	0.06	13.63	< .001	0.64	0.04	17.38	< .001	0.40				
aware	awa1	1.00$^+$				0.82	0.03	27.64	< .001	0.67	0.62	0.66	0.73	2.70
	awa2	1.03	0.06	16.18	< .001	0.84	0.03	28.32	< .001	0.70				
	awa3	0.86	0.05	15.70	< .001	0.70	0.03	20.79	< .001	0.49				
collect	coll1	1.00$^+$				0.82	0.01	61.96	< .001	0.68	0.73	0.89	0.89	8.45
	coll2	0.92	0.02	39.25	< .001	0.76	0.02	48.45	< .001	0.57				
	coll3	1.15	0.02	56.36	< .001	0.95	0.01	128.34	< .001	0.90				
	coll4	1.06	0.02	61.20	< .001	0.88	0.01	88.81	< .001	0.77				
primuse	STPE1	1.00$^+$				0.91	0.01	73.64	< .001	0.83	0.79	0.90	0.92	11.93
	STPE2	0.95	0.02	56.72	< .001	0.87	0.01	82.70	< .001	0.75				
	STPE3	0.97	0.02	58.04	< .001	0.88	0.01	95.98	< .001	0.78				
	STPE4	0.98	0.02	58.36	< .001	0.89	0.01	99.00	< .001	0.79				
privuse	TAU1	1.00$^+$				0.93	0.01	151.88	< .001	0.86	0.88	0.94	0.95	17.30
	TAU2	1.04	0.01	138.23	< .001	0.97	0.00	223.09	< .001	0.93				
	TAU3	1.03	0.01	140.53	< .001	0.95	0.00	205.54	< .001	0.91				
	TAU4	0.97	0.01	102.03	< .001	0.90	0.01	106.90	< .001	0.81				
ease	TAE1	1.00$^+$				0.90	0.01	75.75	< .001	0.81	0.72	0.88	0.89	8.12
	TAE2	0.85	0.02	42.94	< .001	0.77	0.02	50.63	< .001	0.59				
	TAE3	0.97	0.02	50.76	< .001	0.87	0.01	71.99	< .001	0.76				
	TAE4	0.94	0.02	49.38	< .001	0.85	0.01	66.73	< .001	0.72				
bi	STBI1	1.00$^+$				0.95	0.01	189.61	< .001	0.91	0.86	0.93	0.93	13.56
	STBI2	0.95	0.01	100.82	< .001	0.91	0.01	122.42	< .001	0.83				
	STBI4	0.96	0.01	103.36	< .001	0.92	0.01	126.51	< .001	0.84				
results	TAR1	1.00$^+$				0.86	0.01	65.62	< .001	0.74	0.69	0.84	0.85	5.51
	TAR2	0.88	0.02	40.69	< .001	0.76	0.02	49.45	< .001	0.58				
	TAR3	1.00	0.02	44.44	< .001	0.87	0.01	61.83	< .001	0.75				
fc	STFC1	1.00$^+$				0.69	0.02	34.95	< .001	0.48	0.57	0.78	0.82	4.54
	STFC2	1.19	0.04	30.50	< .001	0.83	0.02	52.77	< .001	0.69				
	STFC3	1.14	0.04	25.46	< .001	0.79	0.02	38.96	< .001	0.63				
	STFC4	1.02	0.05	22.04	< .001	0.71	0.02	29.26	< .001	0.50				
trust	STT1	1.00$^+$				0.97	0.00	202.29	< .001	0.93	0.70	0.90	0.91	10.13
	STT2	1.00	0.01	117.14	< .001	0.96	0.00	203.71	< .001	0.93				
	STT3	0.79	0.02	51.18	< .001	0.77	0.02	50.90	< .001	0.59				
	STT4	0.86	0.01	68.35	< .001	0.83	0.01	68.59	< .001	0.69				
	STT5	0.65	0.02	32.22	< .001	0.63	0.02	32.02	< .001	0.40				
	STT6	0.84	0.02	54.06	< .001	0.81	0.01	55.24	< .001	0.65				

Note: $^+$ fixed parameter; the standardized solution is STDALL

equation model on perceived trustworthiness and technology acceptance, that is, hypotheses H_1 thru H_{18} from Section 4.1. Table 6 includes the corresponding near-significant or significant regression coefficients.

Core Technology Acceptance Model. As expected in core TAM, Primary Usefulness, Privacy Usefulness all impact behavioral intention positively. We thereby reject the null hypotheses corresponding to H_{16} and H_{17}. Regarding H_{18}, the impact of ease of use on behavioral intention is statistically significant. Ease of Use has a statistically significant effect on both kinds of Usefulness. Hence, we reject the null hypotheses corresponding to H_{14} and H_{15}. The TAM antecedents of behavioral intention explain $R^2 = 83\%$ of its variance.

TAM Antecedents. Perceived Trustworthiness has a statistically significant impact on both forms of Usefulness. Hence we reject the null hypotheses corresponding to H_{12} and H_{13}. Results Demonstrability has a statistically significantly positive impact on both forms



Note: Restricted to latent variables. Covariances are not shown for visual clarity. Edges with absolute $\beta < 0.10$ are omitted.

Figure 4: Regression path model (standardized β)

Table 6: Coefficients of the regression path model

Relation	H	B	SE	p	β
primuse ~ ctrl***	H_3	-0.314	0.069	< .001	-0.269
primuse ~ aware***	H_3	0.340	0.078	< .001	0.303
primuse ~ collect**	H_3	0.136	0.044	.002	0.123
privuse ~ ctrl***	H_4	-0.247	0.069	< .001	-0.208
privuse ~ aware***	H_4	0.390	0.078	< .001	0.340
privuse ~ collect	H_4	-0.017	0.041	.677	-0.015
primuse ~ fit*	H_5	0.111	0.045	.014	0.099
primuse ~ ts***	H_5	-0.153	0.041	< .001	-0.153
privuse ~ fit***	H_6	0.156	0.043	< .001	0.137
privuse ~ ts**	H_6	-0.107	0.039	.006	-0.105
trust ~ fc***	H_7	1.209	0.048	< .001	0.782
ease ~ fc***	H_8	0.646	0.061	< .001	0.448
primuse ~ results***	H_9	0.268	0.067	< .001	0.253
privuse ~ results***	H_{10}	0.340	0.057	< .001	0.314
ease ~ results***	H_{11}	0.500	0.042	< .001	0.476
primuse ~ trust***	H_{12}	0.436	0.034	< .001	0.465
privuse ~ trust***	H_{13}	0.427	0.031	< .001	0.446
primuse ~ ease	H_{14}	0.003	0.062	.955	0.003
privuse ~ ease	H_{15}	0.048	0.050	.338	0.047
bi ~ primuse***	H_{16}	0.629	0.027	< .001	0.598
bi ~ privuse***	H_{17}	0.226	0.029	< .001	0.220
bi ~ ease***	H_{18}	0.181	0.034	< .001	0.171

of Usefulness as well as Ease of Use. We thereby reject the null hypotheses corresponding to H_9, H_{10} and H_{11}. Facilitating Conditions statistically significantly yielded a positive change in Perceived Trustworthiness and Ease of Use. We reject the null hypotheses corresponding to H_7 and H_8.

How much variance of the endogenous latent variables is explained by the model? The model explains the variance of primary usefulness and privacy usefulness to an extent of $R^2 = 50\%$ and $R^2 = 72\%$, respectively. Similarly, $R^2 = 75\%$ of the variance of Ease of Use is explained. The antecedents of Perceived Trustworthiness explain $R^2 = 61\%$ of its variance.

Attitudes & Subjective Norms. We consider privacy concern first and present a comparison of the situation in indirect and direct modeling in Table **??**. First, we observe that control and awareness have inconsistent impact on their consequences. While ctrl impacts both forms of usefulness negatively, aware impacts them positively. The impact of collection is comparatively small. We could not unequivocally reject the null hypotheses corresponding to the hypotheses (H_1, H_3, H_4) on impact of privacy concerns (IUIPC control, awareness, and collection) on either Usefulness or Intention to Use. The comparison between indirect and direct modeling of Appendix C, shows that the direct effects of ctrl, aware and collect on behavioral intention negate the indirect effects through the perceived usefulness.

We find a similar situation with faith in technology (fit) and trusting stance (ts). Here, faith technology has a positive impact on usefulness and trusting stance a negative impact on usefulness. Likewise, the direct paths to behavioral intention negate these effects.

6.3.2 Impact of ACS Properties. As outlined in Section 4.2, we anticipated intrinsic and presentation properties experimentally manipulated to impact the antecedents of the core technology acceptance model. Table 7 shows the corresponding near-significant and significant coefficients. We note that only the negative impact on perceived trustworthiness was statistically significant.

Table 7: Selected coefficients of the causal SEM, $p < .15$

Relation	H	B	SE	p	β
primuse ~ d_gov	$H_{C,1}$	-0.175	0.112	.118	-0.071
primuse ~ d_company*	$H_{C,1}$	-0.250	0.112	.025	-0.095
trust ~ benefits	$H_{C,2}$	-0.144	0.100	.150	-0.061
primuse ~ usage	$H_{C,3}$	-0.112	0.075	.134	-0.052
primuse ~ simplicity*	$H_{C,4}$	0.203	0.079	.010	0.096
ease ~ simplicity***	$H_{C,4}$	0.423	0.093	< .001	0.201
primuse ~ people	$H_{C,5}$	0.112	0.075	.132	0.054
trust ~ d_contact*	$H_{C,6}$	0.281	0.121	.020	0.103
ease ~ d_contact**	$H_{C,6}$	0.311	0.109	.004	0.120

Intrinsic Properties. The intrinsic properties (provider, benefits and usage) were largely not statistically significant, apart from the provider being set to a company, which had a slight negative impact on primary usefulness. Hence, we failed to reject the null hypotheses corresponding to $H_{C,1}$, $H_{C,2}$ and $H_{C,3}$.

Presentation Properties. The presentation of the ACS (simplicity, people, support) made a considerable difference. Simplicity had the greatest impact on the model, statistically significantly affecting primary usefulness ($\beta = 0.1$) and ease of use ($\beta = 0.2$). We thereby rejected the null hypothesis corresponding to $H_{C,4}$. The total effect of simplicity on the behavioral intention of the users was 0.08.

While the presence of people did not show a statistically significant impact, failing to reject the null hypothesis corresponding to $H_{C,5}$, the other two interventions carried significant weight. In the support category it made statistically significant difference to

have a contact option, affecting both trust and ease of use positively on the order of $\beta \approx 0.1$. Hence, we rejected the null hypothesis corresponding to $H_{C,6}$.

7 DISCUSSION

7.1 Technology acceptance of ACS

We can reliably explain how users adapt Attribute-Based Credential Systems. The extended Technology Acceptance Model we proposed in this study is an excellent fit. The model predicts the user's intention to adapt ACS very well: The antecedents of behavioral intention explain $R^2 = 83\%$ of its variance.

Perceived trustworthiness is a major predictor of both primary usefulness and privacy usefulness with medium standardized effects. We expect these effect magnitudes to relevant for practice. Benenson et al. [4] did not incorporate privacy concern into the model and measured perceived trust only as a single Likert item, limiting its reliability. Compared to the works of Benenson et al. [4] and Harborth and Pape [35], we believe that including perceived trustworthiness was a sound choice over using risk and trust beliefs. In contrast to that earlier work, we offer a large-scale study with a UK-representative sample and rigorous modeling for ordinal, non-normal data.

7.2 Primary usefulness rules

Primary usefulness trumps privacy usefulness and ease of use. It is the strongest predictor of behavioral intention to adapt an ACS. This means that it matters most to users that an ACS is useful in their daily lives, supports their productivity, increases the chances to fulfill primary tasks and helps to achieve primary tasks more quickly. The impact of privacy usefulness, that is, to what extent the ACS helps protecting the user's privacy, is less than half that impactful. Thereby we can confirm a common belief in the community that the user's focus is on the primary task and not on the secondary task of privacy protection. Our observations here are aligned with Benenson et al. [4].

While the effect of ease of use was in the same order of magnitude as privacy usefulness in our study, we expect that its role will be mode pronounced when users interact with actual artifacts, such as a smart cards or cell phone apps.

Lesson Learned 1 (Do not impede the primary task). *Software developers best establish what users seek to achieve in their daily life and design the ACS to support them in this endeavor. At the very least, they would need to make sure the ACS does not get in the way. For example, both the tight integration of Tor Browser compared to other user interfaces [18] and the seamless use of the Privacy Pass [20] make it more likely that the PETs are adopted.*

7.3 Usefulness mediates the impact of privacy concern

Our mediation analysis in Appendix C highlighted that there exists a significant partial mediation of privacy concern through both variants of usefulness. The mediation of awareness and control as causes of behavioral intention was quite strong: Usefulness mediates a proportion of approximately 46% of the impact of both privacy concern factors on behavioral intention. This is not just a modeling artifact, but informs steps to take: Perceived usefulness of an ACS will play a role in how users take action on their privacy concerns.

Lesson Learned 2 (Usefulness enables action on privacy concern). *We recommend that developers and providers optimize ACS perceived usefulness both for primary tasks and for privacy protection. If the perceived usefulness is low, users' impetus to act on their privacy concerns will be disproportionately diminished. For example, we would consider the approach of IRMA Card [23, 59] a success model: focus on simple, useful scenarios with meaningful privacy protection for the users, such as selective disclosure.*

7.4 Facilitating conditions and demonstrable results are key drivers

While perceived trustworthiness is a major antecedent of both types of usefulness, more than 60% of its variance is explained by other factors. Therefore, it is crucial to evaluate what impacts user's perceived trustworthiness apart from the pedigree of the ACS. Here, facilitating conditions and results demonstrability come into play. While facilitating conditions model to what extent a user has access to an adequate support framework, results demonstrability establishes to what extent the user can explain the outcomes and benefits of using the ACS.

Facilitating conditions strongly impact trust and ease of use. Does the user have access to the right resources and knowledge, compatible systems and help? It stands to reason that these questions indeed need to be answered well to convince a user to adopt an ACS.

Results demonstrability indicates whether the results are apparent to the user and whether the user is capable of explaining the results to others. It yields considerable effects on ease of use and privacy usefulness. While both facilitating conditions and demonstrable results had consistently positive effects as drivers of behavioral intention, the total effect of facilitating conditions was about twice as strong as demonstrable results.

Lesson Learned 3 (Help users run and understand the ACS). *Once providers established an ACS that gets the job done in a trustworthy way, the next priority is establishing strong support framework that provides further resources and knowledge, robust compatibility, and help. Enable the user's understanding of the results and consequences of using the ACS. Ideally, an ACS would be compatible with a wide range of desktop and mobile operating systems, integrate seamlessly, and come both with copious support and education options. For example, early ACS such as IBM Identity Mixer and Microsoft U-Prove were largely supported by technical documentation written by engineers and researchers, but provided little support for end users.*

7.5 Make it simple!

Of the manipulated variables, simplicity has the most consistent positive effect: We found that choosing simple language in terms of Flesh readability had significant positive effects on primary usefulness and ease of use. Hence, easy to understand language makes users more likely to adopt the technology. While the total effect of simplicity was quite small (half the magnitude of demonstrable results) readability can be achieved with little effort but will impact

the user's grasp of the support available and of the understanding what the ACS does.

We recommend that software developers and identity providers fine-tune how to present an ACS in a simple fashion while still convincing users of its merits: Having too little privacy and technical content could diminish perceived trustworthiness and usefulness.

Lesson Learned 4 (Present the ACS as simple as possible.). *Identity providers can further boost uptake by making sure that the ACS description is in plain English and fairly easy to read (Flesh readability greater than 60). It is advisable to still explain technical aspects and privacy protection to support the users' perception of trustworthiness and privacy usefulness.*

7.6 Lessons learned for the privacy paradox

Understanding how the users' privacy concerns impact their intention to act is crucial to explain the privacy paradox. While earlier research pointed out that unreliable privacy concern scales attenuate the impact we can see on behavior, we gain further insights from this study.

7.6.1 Mediation matters. While we have shown in Section 7.3 that perceived usefulness mediates the impact of privacy concern on behavioral intention, this vouches for further discussion. We expect, in general, that mediation is an important concern in the investigation of the privacy paradox.

We analyzed the indirect and direct paths of privacy concern impacting behavioral intention. Here, we observed an inconsistent mediation for all privacy concern factors discussed in Appendix C, that is, that direct effects and indirect effects have different signs. For example, control yields a positive effect through a direct path to behavioral intention, but a negative effect through indirect paths mediated by perceived usefulness. As a consequence, the total effect of privacy concern on behavioral intention is quite small. The inconsistent mediation could be a previously unexplored cause of the privacy paradox and vouches for a thorough investigation beyond the scope of this paper.

7.6.2 Inconsistent impact of privacy concern factors. We observed that the privacy concern factors control and awareness have inconsistent effects on behavioral intention. While awareness increases the behavioral intention to use the ACS, control diminishes it. Awareness emphasizes that the user be aware and knowledgable how information is used and that companies facilitate that by clearly disclosing how they handle information. Control on the other hand emphasizes the right to control and autonomy over decisions over the user's information. One may hypothesize that the conviction that the user has the right to control already yields less behavioral intention to adopt further privacy preserving technologies to enforce that control. The inconsistency between effects of privacy concern factors on behavioral intention offers an alternative explanation why the privacy paradox occurs: The effects of different privacy concern factors cancel each other out. Overall, the observations on mediation will add to the methodological concerns in the investigation of the privacy paradox already summarized by Kokolakis [37].

Lesson Learned 5 (The paradox is in the details). *We recommend that researchers constructing models in the realm of the privacy paradox scrutinize mediations: (i) Investigate mediations between privacy concern and behavior as a matter of course. (ii) Take into account the impact of individual privacy concern factors as opposed to modeling privacy concern as a compound score without further examination. (iii) Beware of inconsistent mediations and inconsistent effects of privacy concern factors. While Dienlin and Trepte [24] put a considerable emphasis on mediation, a range of other studies in the field brushed over this aspect.*

7.7 Limitations

7.7.1 Ecological Validity. There are limitations to the ecological validity as the ACS Web pages used as stimuli were mock-ups. With respect to manipulating the provider, the Web sites did not use the provider's logos or domains due to licensing and legal restrictions. Otherwise, they mimicked the look-and-feel of existing sites of providers on Attribute-Based Credential Systems.

In order to gain a large representative sample and to be able to manipulate aspects of the ACS Web site, we struck a balance in terms of ecological validity. The study of Benenson et al. [4] was more hands-on in offering their students physical artifacts (smart cards, etc.), thereby yielding stronger ecological validity.

7.7.2 Generalizability. The large sample was representative for the UK, in terms of age, gender and ethnicity. Due how Prolific operates, the sampling process is judgment sampling with self-selection, rather than a random sampling process on UK residents. However, this study offered a better population representativeness and diversity than prior works [4, 34] and afforded us stronger generalizability on these grounds.

The sample for the study was drawn in 2019 before the Covid-19 pandemic. While security and privacy attitudes may have changed after the pandemic, we are confident that the relative strengths of effect sizes will stay consistent, e.g., that results demonstrability and facilitating conditions will impact adoption positively.

7.7.3 Measurement of Privacy Concerns. As indicated in the background section and observed in earlier studies [30, 31], the reliability of IUIPC-10 as measurement of privacy concern is limited. As a consequence, we face a low signal-to-noise ratio on the privacy concern measurement and an attenuation of its effects on other factors. While most of the relations could still be estimated with considerable certainty, we incurred lower certainty for smaller regression coefficients.

8 CONCLUSION

We established the first WLSMV-estimated comprehensive structural latent variable model for the trustworthiness and acceptance of Attribute-Based Credential System (ACS) and built a sound foundation for research in user decision making on ACS. Based on a large sample representative of the UK population in gender, age and ethnicity, we are able to show that an extended Technology Acceptance Model is a sound representation of user decision making. Our model explains twice the variance of user behavioral intention of adoption compared to earlier work [34, 35].

We gained new insights which factors impact the users decisions: We are the first to include facilitating conditions and results

demonstrability as key drivers and show that they yield a consistent positive effect on the ultimate technology acceptance of ACS. Overall, our model constitutes a sound nomological network that can be used for other privacy-enhancing technologies beyond the given use case of ACS.

Furthermore, we have established the first cause-effect analysis of the impact of intrinsic and presentation properties on technology acceptance. There, we could show that simplicity of content yields a consistent positive impact: Using simple language to instruct users on facilitating conditions, that is, what knowledge and resources are needed to run the ACS successfully, and on demonstrable results, that is, what the ACS does in day-to-day and how to convey that to others, will yield a positive impact on technology acceptance. Therefore, we highlight the credo "Simply tell me how." as instrumental for technology adoption.

Our work, finally, offers new methodological considerations into the study of the privacy paradox beyond the existing reviewed work [37]: (i) We observed inconsistent effects of different factors making up privacy concern: While stronger awareness attitude amplified the intention to use the ACS, stronger control attitude diminished the intention to use. Studies that model privacy concern monolithically as one factor will suffer from these two forces competing with each other and, thereby, leaving privacy behavior unexplained. (ii) We could show that perceived usability yielded a partial mediation of privacy concern factors on behavioral intention. (iii) We found an inconsistent mediation when investigating indirect and direct effects of privacy concern, diminishing the overall effect on behavioral intention. We recommend scrutinizing mediations between privacy concern and behavioral intention in future work. Overall, we believe that this work will make an informative addition to the body of research on human factors in privacy research and of privacy-enhancing technologies.

ACKNOWLEDGMENTS

This work was supported by ERC Starting Grant CASCAde (GA n°716980).

REFERENCES

[1] Ali Abdallah Alalwan, Yogesh K Dwivedi, and Nripendra P Rana. 2017. Factors influencing adoption of mobile banking by Jordanian bank customers: Extending UTAUT2 with trust. International Journal of Information Management 37, 3 (2017), 99–110.

[2] James C Anderson and David W Gerbing. 1988. Structural equation modeling in practice: A review and recommended two-step approach. Psychological bulletin 103, 3 (1988), 411.

[3] Yakov Bart, Venkatesh Shankar, Fareena Sultan, and Glen L Urban. 2005. Are the drivers and role of online trust the same for all web sites and consumers? A large-scale exploratory empirical study. Journal of marketing 69, 4 (2005), 133–152.

[4] Zinaida Benenson, Anna Girard, and Ioannis Krontiris. 2015. User Acceptance Factors for Anonymous Credentials: An Empirical Investigation. In WEIS.

[5] Zinaida Benenson, Anna Girard, Ioannis Krontiris, Vassia Liagkou, Kai Rannenberg, and Yannis Stamatiou. 2014. User acceptance of privacy-ABCs: an exploratory study. In International Conference on Human Aspects of Information Security, Privacy, and Trust. Springer, 375–386.

[6] Patrik Bichsel, Jan Camenisch, Thomas Groß, and Victor Shoup. 2009. Anonymous credentials on a standard java card. In Proceedings of the 16th ACM conference on Computer and communications security. 600–610.

[7] Kenneth A Bollen and Jersey Liang. 1988. Some properties of Hoelter's CN. Sociological Methods & Research 16, 4 (1988), 492–503.

[8] James A Bovaird and Natalie A Koziol. 2012. Measurement models for ordered-categorical indicators. In Handbook of Structural Equation Modeling, Rick H. Hoyle (Ed.). The Guilford Press, 495–511.

[9] Stefan Brands. 2000. Rethinking public key infrastructures and digital certificates: building in privacy. Mit Press.

[10] Oliver B Büttner and Anja S Göritz. 2008. Perceived trustworthiness of online shops. Journal of Consumer Behaviour: An International Research Review 7, 1 (2008), 35–50.

[11] Jan Camenisch and Thomas Groß. 2008. Efficient attributes for anonymous credentials. In Proceedings of the 15th ACM conference on Computer and communications security. ACM, 345–356.

[12] Jan Camenisch and Anna Lysyanskaya. 2002. Dynamic accumulators and application to efficient revocation of anonymous credentials. In Annual International Cryptology Conference. Springer, 61–76.

[13] Jan Camenisch and Anna Lysyanskaya. 2002. A signature scheme with efficient protocols. In International Conference on Security in Communication Networks. Springer, 268–289.

[14] Jan Camenisch and Anna Lysyanskaya. 2004. Signature Schemes and Anonymous Credentials from Bilinear Maps. In Advances in Cryptology – CRYPTO 2004, Matt Franklin (Ed.). Springer Berlin Heidelberg, Berlin, Heidelberg, 56–72.

[15] Jan Camenisch and Els Van Herreweghen. 2002. Design and implementation of the idemix anonymous credential system. In Proceedings of the 9th ACM conference on Computer and communications security. 21–30.

[16] Melissa Chase, Trevor Perrin, and Greg Zaverucha. 2019. The Signal Private Group System and Anonymous Credentials Supporting Efficient Verifiable Encryption. Technical Report. Cryptology ePrint Archive, Report 2019/1416.

[17] David Chaum. 1985. Security without identification: Transaction systems to make big brother obsolete. Commun. ACM 28, 10 (1985), 1030–1044.

[18] Jeremy Clark, Paul C Van Oorschot, and Carlisle Adams. 2007. Usability of anonymous web browsing: an examination of tor interfaces and deployability. In Proceedings of the 3rd symposium on Usable privacy and security. 41–51.

[19] Cynthia L Corritore, Robert P Marble, Susan Wiedenbeck, Beverly Kracher, and Ashwin Chandran. 2005. Measuring online trust of websites: Credibility, perceived ease of use, and risk. AMCIS 2005 proceedings (2005), 370.

[20] Alex Davidson, Ian Goldberg, Nick Sullivan, George Tankersley, and Filippo Valsorda. 2018. Privacy pass: Bypassing internet challenges anonymously. Proceedings on Privacy Enhancing Technologies (2018).

[21] Fred D Davis. 1989. Perceived usefulness, perceived ease of use, and user acceptance of information technology. MIS quarterly (1989), 319–340.

[22] Fred D Davis, Richard P Bagozzi, and Paul R Warshaw. 1989. User acceptance of computer technology: a comparison of two theoretical models. Management science 35, 8 (1989), 982–1003.

[23] Antonio De La Piedra, Jaap-Henk Hoepman, and Pim Vullers. 2014. Towards a full-featured implementation of attribute based credentials on smart cards. In International Conference on Cryptology and Network Security. Springer, 270–289.

[24] Tobias Dienlin and Sabine Trepte. 2015. Is the privacy paradox a relic of the past? An in-depth analysis of privacy attitudes and privacy behaviors. European journal of social psychology 45, 3 (2015), 285–297.

[25] Christine DiStefano. 2002. The impact of categorization with confirmatory factor analysis. Structural equation modeling 9, 3 (2002), 327–346.

[26] Florian N Egger et al. 2001. Affective design of e-commerce user interfaces: How to maximise perceived trustworthiness. In Proc. Intl. Conf. Affective Human Factors Design. Citeseer, 317–324.

[27] David Gefen. 2002. Reflections on the dimensions of trust and trustworthiness among online consumers. ACM SIGMIS Database: the DATABASE for Advances in Information Systems 33, 3 (2002), 38–53.

[28] Nina Gerber, Paul Gerber, and Melanie Volkamer. 2018. Explaining the privacy paradox: A systematic review of literature investigating privacy attitude and behavior. Computers & Security 77 (2018), 226–261.

[29] Thomas Groß. 2015. Signatures and Efficient Proofs on Committed Graphs and NP-Statements. In Financial Cryptography and Data Security, Rainer Böhme and Tatsuaki Okamoto (Eds.). Springer Berlin Heidelberg, Berlin, Heidelberg, 293–314.

[30] Thomas Groß. 2021. Validity and Reliability of the Scale Internet Users' Information Privacy Concern (IUIPC). Proceedings of the Privacy-Enhancing Technologies Symposium (PoPETS) 2021, 2 (2021), 235–258.

[31] Thomas Groß. 2023. Toward Valid and Reliable Privacy Concern Scales: The Example of IUIPC-8. In Human Factors in Privacy Research. Springer Verlag, 55–81.

[32] Joe F Hair Jr, Lucy M Matthews, Ryan L Matthews, and Marko Sarstedt. 2017. PLS-SEM or CB-SEM: updated guidelines on which method to use. International Journal of Multivariate Data Analysis 1, 2 (2017), 107–123.

[33] Marian Harbach, Sascha Fahl, Matthias Rieger, and Matthew Smith. 2013. On the acceptance of privacy-preserving authentication technology: the curious case of national identity cards. In Privacy Enhancing Technologies: 13th International Symposium, PETS 2013, Bloomington, IN, USA, July 10-12, 2013. Proceedings 13. Springer, 245–264.

[34] David Harborth and Sebastian Pape. 2018. Examining technology use factors of privacy-enhancing technologies: the role of perceived anonymity and trust. In Twenty-fourth Americas Conference on Information Systems. New Orleans.

[35] David Harborth and Sebastian Pape. 2020. How privacy concerns, trust and risk beliefs, and privacy literacy influence users' intentions to use privacy-enhancing technologies: The case of Tor. ACM SIGMIS Database: The DATABASE for Advances in Information Systems 51, 1 (2020), 51–69.
[36] Rex B Kline. 2015. Principles and practice of structural equation modeling (4th ed. ed.). The Guilford Press.
[37] Spyros Kokolakis. 2017. Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon. Computers & security 64 (2017), 122–134.
[38] Ioannis Krontiris, Zinaida Benenson, Anna Girard, Ahmad Sabouri, Kai Rannenberg, and Peter Schoo. 2016. Privacy-ABCs as a case for studying the adoption of PETs by users and service providers. In Privacy Technologies and Policy: Third Annual Privacy Forum, APF 2015, Luxembourg, Luxembourg, October 7-8, 2015, Revised Selected Papers 3. Springer, 104–123.
[39] Matthew KO Lee and Efraim Turban. 2001. A trust model for consumer internet shopping. International Journal of electronic commerce 6, 1 (2001), 75–91.
[40] Younghwa Lee, Kenneth A Kozar, and Kai RT Larsen. 2003. The technology acceptance model: Past, present, and future. Communications of the Association for information systems 12, 1 (2003), 50.
[41] Torrin M Liddell and John K Kruschke. 2018. Analyzing ordinal data with metric models: What could possibly go wrong? Journal of Experimental Social Psychology 79 (2018), 328–348.
[42] David P MacKinnon, Amanda J Fairchild, and Matthew S Fritz. 2007. Mediation analysis. Annu. Rev. Psychol. 58 (2007), 593–614.
[43] Naresh K Malhotra, Sung S Kim, and James Agarwal. 2004. Internet users' information privacy concerns (IUIPC): The construct, the scale, and a causal model. Information systems research 15, 4 (2004), 336–355.
[44] Kieran Mathieson. 1991. Predicting user intentions: comparing the technology acceptance model with the theory of planned behavior. Information systems research 2, 3 (1991), 173–191.
[45] D Harrison Mcknight, Michelle Carter, Jason Bennett Thatcher, and Paul F Clay. 2011. Trust in a specific technology: An investigation of its components and measures. ACM Transactions on Management Information Systems (TMIS) 2, 2 (2011), 12.
[46] Daniel M Oppenheimer, Tom Meyvis, and Nicolas Davidenko. 2009. Instructional manipulation checks: Detecting satisficing to increase statistical power. Journal of Experimental Social Psychology 45, 4 (2009), 867–872.
[47] Paul A Pavlou. 2003. Consumer acceptance of electronic commerce: Integrating trust and risk with the technology acceptance model. International journal of electronic commerce 7, 3 (2003), 101–134.
[48] Sören Preibusch. 2013. Guide to measuring privacy concern: Review of survey and observational instruments. International Journal of Human-Computer Studies 71, 12 (2013), 1133–1143.
[49] Ahmad Sabouri. 2015. Understanding the determinants of privacy-ABC technologies adoption by service providers. In Open and Big Data Management and Innovation: 14th IFIP WG 6.11 Conference on e-Business, e-Services, and e-Society, I3E 2015, Delft, The Netherlands, October 13-15, 2015, Proceedings 14. Springer, 119–132.
[50] Ahmad Sabouri. 2016. On the user acceptance of privacy-preserving attribute-based credentials–a qualitative study. In Data Privacy Management and Security Assurance: 11th International Workshop, DPM 2016 and 5th International Workshop, QASA 2016, Heraklion, Crete, Greece, September 26-27, 2016, Proceedings 11. Springer, 130–145.
[51] Dexin Shi, Alberto Maydeu-Olivares, and Yves Rosseel. 2020. Assessing fit in ordinal factor analysis models: SRMR vs. RMSEA. Structural Equation Modeling: A Multidisciplinary Journal 27, 1 (2020), 1–15.
[52] H Jeff Smith, Sandra J Milberg, and Sandra J Burke. 1996. Information privacy: measuring individuals' concerns about organizational practices. MIS quarterly (1996), 167–196.
[53] Daniel J Solove. 2021. The myth of the privacy paradox. Geo. Wash. L. Rev. 89 (2021), 1.
[54] Bernadette Szajna. 1996. Empirical evaluation of the revised technology acceptance model. Management science 42, 1 (1996), 85–92.
[55] Syh-Yuan Tan and Thomas Groß. 2020. MoniPoly—An Expressive q-SDH-Based Anonymous Attribute-Based Credential System. In ASIACRYPT 2020.
[56] Syh-Yuan Tan and Thomas Groß. 2023. A Relational Credential System from q-SDH-based Graph Signatures. Cryptology ePrint Archive Report 2023/1181. IACR.
[57] Viswanath Venkatesh and Fred D Davis. 2000. A theoretical extension of the technology acceptance model: Four longitudinal field studies. Management science 46, 2 (2000), 186–204.
[58] Viswanath Venkatesh, James YL Thong, and Xin Xu. 2012. Consumer acceptance and use of information technology: extending the unified theory of acceptance and use of technology. MIS quarterly (2012), 157–178.
[59] Pim Vullers and Gergely Alpár. 2013. Efficient selective disclosure on smart cards using idemix. In IFIP Working Conference on Policies and Research in Identity Management. Springer, 53–67.

A OPERATIONALIZATION

We give a detailed account how questionnaires introduced as materials were set up as variables for Structural Equation Modelling. First, we shall consider the measurement instruments in Section A.1. Second, we will introduce the manipulations for different experiment conditions. And, finally, we explain the instructional manipulation checks used in Section A.3.

A.1 Measurement Instruments

We adapted a range of standard questionnaires for the topic of Attribute-Based Credential Systems as target technologies. The overall purpose was to measure system trustworthiness and technology acceptance contextualized by privacy concerns and general faith in technology. Specifically, we selected the following instruments and offer an overview of the measurement variables in Table 1:

Privacy concerns (IUIPC-10) [43] Elicits the long-term privacy concerns of users in the dimensions control (ctrl), awareness (aware) and collection (collect).

Faith in Technology (FIT) [45] Elicits long-term attitudes on using technology and general trusting stance. We selected FIT as a covariate informing primary usefulness.

System Trustworthiness (ST) [45] Elicits perceived trustworthiness in a particular technology, with a range of sub-scales. (i) Social influence (si) elicits a subjective norm in the form perceived social pressure to engage or not to engage in a behavior. (ii) Facilitating conditions (fc) models the available resources, knowledge and support engage with the technology to be trusted. (iii) Performance Expectancy measures the expectation that the technology will be useful, which we used as primary usefulness (primuse) in the Technology Acceptance Model (TAM 2.0). (iv) Perceived Trustworthiness (trust) elicits to what extent participants are willing to trust the technology. (v) Behavioral Intention models is identical to the behavioral intention used in TAM 2.0.

Technology Acceptance Model (TAM 2.0) [57] Models to what extent users are willing to adopt a given technology. (i) Results Demonstrability (results) models whether participants find the results apparent and easily communicable. (ii) Primary Usefulness (primuse) measures the expectation that the technology will be useful in general, adapted from ST Performance Expectancy. (iii) Privacy Usefulness (privuse) elicits whether participants find the technology useful to support their privacy. (iv) Behavioral Intention (bi) models the intent to use the technology, which is identical to the behavioral intention used in ST.

Instrument Evaluation and Empirical Refinement. As we have adapted existing questionnaires in their wording to match them to the application area of Attribute-Based Credential System, we diligently evaluated the final instruments for their validity and reliability.

Overall, the instruments used yielded considerable validity and reliability metrics. For the TAM Results Demonstrability construct, we found that one item (rTAR4) was inconsistent with the rest of the construct and chose to eliminate this item, with no ill effect on

the reliability of the measurement of the construct. We removed the Social influence (si) subscale, because of excessively great indicator correlation. With regards to behavioral intention, we removed STBI3 due to great correlation with STBI1.

We noticed that two IUIPC sub-scales (ctrl and aware) yielded low internal consistency ω as discussed in earlier work. We chose to retain these constructs to keep privacy concerns in the model.

A.2 Manipulations

We developed a Web site about a new Attribute-Based Credential System (ACS), in which different pieces of content could be changed easily. In that, we enabled the manipulation of ACS intrinsic properties—their provider, usage and claimed benefits—and ACS presentation properties—simplicity of the content in terms of readability, presence of people and level of support. The intrinsic properties were changed in the core content, the presentation properties also in the Web design elements around the core content. These manipulations were to some extent influenced by the work of Egger et al. [26] on affective design of e-commerce user interfaces and design features that yield perceived trustworthiness. Figure 2 illustrates the manipulated pieces of content in the example of a single Web page. We controlled the possible confounder of readability with Flesch's Reading Ease, crafting the text fragments such that they are similar in readability even if they differed in content.

Intrinsic Properties.

(i) provider: intrinsic properties of the provider, manipulated by which provider is being used, incl. a description of the organization in an about section. Four levels (with three binomial dummy variables):
   1. gov: the UK government (d_gov = 1),
   2. company: IBM (an internationally operating company which predominately developed Attribute-Based Credential Systems in the past) (d_company = 1),
   3. uni: a nationally known university (anonymized for submission) in the UK (d_uni = 1).
   4. none: no provider is named, a condition reserved for the presentation trial (d_gov = 0 & d_company = 0 & d_uni = 0).

(ii) benefits: intrinsic benefits of an Attribute-Based Credential System, with two levels:
   1. privacy: general benefits for privacy and data protection (benefits = 0)
   2. user: benefits specific for a user's life (benefits = 1),

(iii) usage: description of how the system is used intrinsically, with two levels:
   1. tech: Usage described in terms of the processes and procedures of the technology (usage = 0),
   2. everyday: Usage described in terms of every-day use of the system (usage = 1).

We define as reference category: university-privacy-tech.

Presentation Properties.

(i) simplicity: simplicity of the language used to convey the usage and benefits of the ACS controlled by readability metrics. Two levels:
   1. complex: employs language being complex, that is, a low readability in terms of Flesch Reading Ease (or correspondingly a high reading grade level) (simplicity =0),
   2. simple: employs simple language, that is, a high readability in terms of Flesch Reading Ease (and low reading grade level) (simplicity = 1).

(ii) people: presentation of the ACS with a photo of a person to relate to or not, with two levels:
   1. nophoto: a photo of a person to relate to is absent (people = 0).
   2. photo: a (stock) photo representing a leading developer is displayed next to the content (people = 1),

(iii) support: presentation of different levels of support opportunities on the Web site. Three levels (with two binomial dummy variables):
   1. fullsupport: support information containing contact information (e-mail and chat) as well as a user feedback system (d_fullsupport = 1),
   2. contact: support information contains contact information only (e-mail and chat) (d_contact = 1),
   3. nosupport: no support-related cues are given (d_fullsupport = 0 & d_contact = 0).

We define as *reference categories*: complex-nophoto-nosupport.

A.3 Manipulation and Attention Checks

We integrated three kinds of manipulation checks in the survey:

1. Factual manipulation checks, asking participants questions about facts of the inspected Web pages, such as, the color of the download button, or presence of manipulations, such as, the presence/absence of a photo as indicated by the condition.
2. Impact manipulation checks, debriefing self-report of the participants how much they perceived a particular aspect of the Web page influenced them.
3. Instructional Manipulation Checks (IMCs) [46], instructions to select a particular option as confirmation of sustained attention.

We pre-registered the plan to remove observations of participants who failed more than one attention check (IMC).

B STRUCTURAL EQUATION MODEL

The nomological network is theoretically founded on the Technology Acceptance Model (TAM 2.0) [57]. It is empirically substantiated taking into account the correlation analysis of Benenson et al. [4]. We depicted the nomology designed for this study in Figure 1.

As summarized in Table 8, we establish the structural equation model in three steps. 1. The *measurement model* is constructed by setting the measurement variables (MVs) defined in the operationalization of Table 1 as reflective measurements of the corresponding latent variables. 2. The *regression path model* is based on the theoretical nomology proposed in Section 4, incorporating the variables primary usefulness (primuse), privacy usefulness (privuse), and ease of use (ease) forming the core of TAM. Results demonstrability (results) and facilitating conditions (fc) act as major antecedents. 3. The *causal path model* is built by adding experimental causes as dichotomous variables (dummy variables for multinomial variables). We incorporated them as regression antecedents for perceived trustworthiness (trust), primary usefulness (primuse), privacy usefulness (privuse), and ease of use (ease). This model also incorporates

Table 8: SEM Modelling Phases

Model	Description
1. Measurement	Reflective measurement of latent variables (LVs) by the measurement variables (MVs, indicators); no regression equations.
2. Regression	Path model incorporating the measurement model plus regression equations according to statistical hypotheses from aims establishing ACS Trustworthiness and Acceptance (§4.1; Figure 1).
3. Causal	Path model incorporating the regression model plus regression equations on dichotomous variables modelling the experiment conditions and, thereby, the causal impact of intrinsic and presentation properties (§4.2).

the download behavior as endogenous dichotomous variable and consequence of behavioral intention.

B.1 Modelling Approach

We followed a modelling approach that embeds the Two-Step Modelling approach proposed by Anderson and Gerling [2] and advocated by Kline [36]. We base the SEMs on a Weighted Least Square estimation with mean and variance correction (WLSMV) to account for the ordinal, non-normal data [8], evaluating the fit with the robust CFI and TLI, a robust RMSEA and SRMR[3]. We compare nested models with the likelihood-ratio test (LRT) on the equal-fit hypothesis. For unnested models, we compare the cn_{05}, that is, the critical N for the χ^2 test at .95 confidence [7], in addition to other fit indices. We proceed according to three steps outlined in Table 8.

(1) We started with the model predicted in aims (Figure 1) theoretically grounded in the general Technology Acceptance Model 2.0 [57] and the model proposed by Benenson et al. [4]
(2) We computed univariate histograms and density diagrams for the inputs to diagnose distribution problems as well as covariance/correlation matrices to indicate variables with risk of substantial multicollinearity. In this process, we identified variables that need additional consideration in the final model.
(3) We evaluated the measurement model first (Table 8, Step 1.), that is, computed a confirmatory factor analysis (CFA) model that only included the exogenous and endogenous latent variables (LVs) for the desired constructs and their indicator/measurement variables (MVs). In that, we established general fit, the significance of all reflective MV-LV relations, as well as factor loadings and the reliability in terms internal consistency.
(4) Based on this analysis, we diagnosed faults in the measurement model and underlying questionnaires, deriving a refined measurement model.
(5) We added the predicted regression equations to the measurement model to build the regression path model (Table 8, Step 2.). We tested with a χ^2 likelihood ratio test (LRT) that the improvement of the more complex regression model over the simpler measurement model is statistically significant. We then expanded the regression path model with direct paths from the attitudes and subjective norms to the behavioral intention (corresponding to H_1 and H_2). We tested this expansion, in turn, with an LRT.
(6) Once convinced that the regression path model is a good fit, we expanded it by dichotomous variables designating the conditions of the experiments, forming the causal path model (Table 8, Step 3.). We tested the statistical significance of incorporating the direct paths on attitudes and subjective norms with an LRT.

[3]Shi et al [51] cautioned that RMSEA is less reliable in WLSMV estimation than usually expected and recommend to focus on the more robust SRMR.

C MEDIATION ANALYSIS

We incorporated a mediation analysis in the step-by-step modeling of ACS technology acceptance, considering both complete and partial mediation. The body of the paper focuses on a complete mediation model, that is, that the impact of privacy concern on behavioral intention is fully mediated by perceived usefulness. This is because the complete mediation model is easier to interpret given the inconsistent mediation we discuss below.

In this appendix, we include the partial mediation model in comparison, that is, that privacy concern impacts behavioral intention both indirectly through the mediation perceived usefulness as well as directly.

For the meditation analysis, we established the regression path model itself in two steps: by first computing a model without the direct paths between subjective norms/attitudes and behavioral intention, that is, excluding the test of H_1 and H_2, and then adding these paths in model building. This first model assumes a complete mediation in that the direct paths are set to zero. The hypothesized partial mediation model includes the paths representing hypotheses H_1 and H_2. This partial mediation model fits statistically significantly better than the complete mediation model model: we rejected the equal-fit hypothesis, $\chi^2(5) = 78.199, p < .001$.

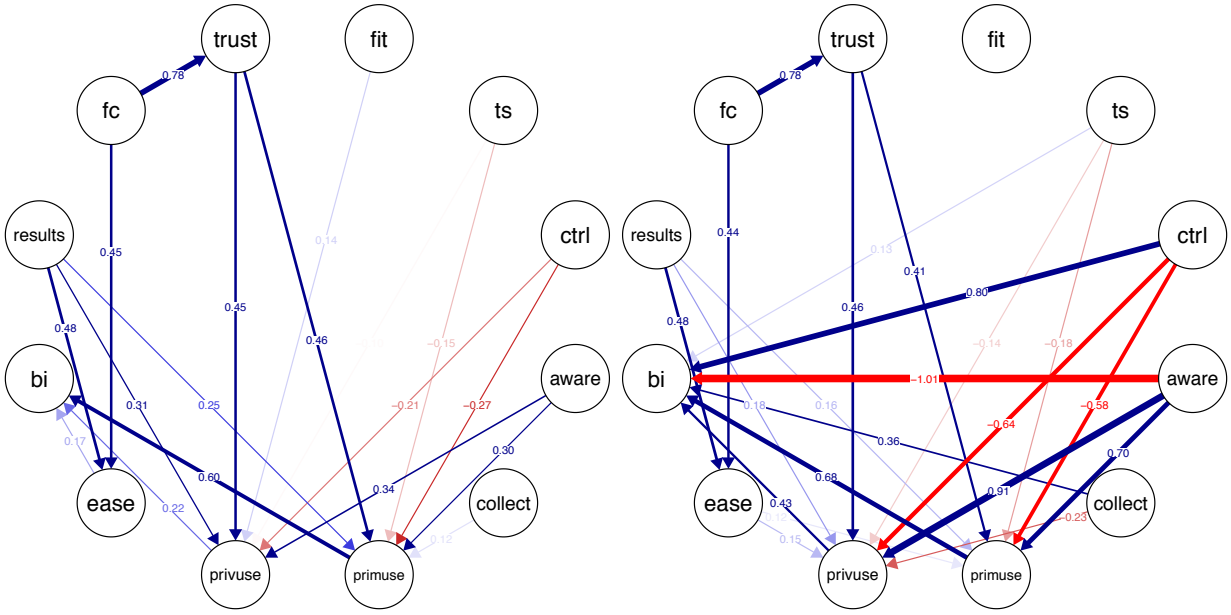
Regarding the causal model, we also compared the complete mediation model to the partial mediation model. We found that the partial mediation model improved the global fit statistically significantly, $\chi^2(5) = 83.791, p < .001$. Both the complete and partial mediation models exhibited excellent fit fulfilling the RMSEA close-fit hypothesis, $p_{\epsilon_0 \leq .05} = .310$ and $p_{\epsilon_0 \leq .05} = .590$, respectively.

We visualize both mediation models in Figure 5 and outline the corresponding effects of privacy concern in Table 9. The table compares the standardized coefficients β of privacy concern factors with respect to their impact on behavioral intention. The left-hand model, called "complete mediation" (cf. Figure 5a), only incorporates the indirect effects of privacy concern through perceived usefulness. The right-hand model, called "partial mediation" (cf. Figure 5b), incorporates a direct path from privacy concern factors to behavioral intention. Of the two models, the partial mediation model is a statistically significantly better fit, $\chi^2(5) = 78.199, p < .001$. We observe an inconsistent mediation: the direct effect yields a different sign than the indirect effect mediated through perceived usefulness. The direct effects have a greater absolute magnitude than the sum of the indirect effects.

Table 9: Privacy concern in complete and partial mediation models.

	complete mediation				partial mediation			
Effect	β	SE	p	95% CI	β	SE	p	95% CI
Indirect Effect $(a * b)$								
ctrl	-0.206	0.040	< .001	[-0.286, -0.127]	-0.673	0.109	< .001	[-0.887, -0.459]
aware	0.256	0.047	< .001	[0.165, 0.347]	0.867	0.136	< .001	[0.600, 1.133]
collect	0.718	0.051	< .001	[0.618, 0.819]	0.541	0.092	< .001	[0.361, 0.721]
Direct Effect c								
ctrl$^+$					0.797	0.140	< .001	[0.523, 1.071]
aware$^+$					-1.006	0.176	< .001	[-1.351, -0.660]
collect$^+$					0.355	0.077	< .001	[0.205, 0.506]
Total Effect								
ctrl	-0.206	0.040	< .001	[-0.286, -0.127]	0.124	0.092	.177	[-0.056, 0.304]
aware	0.256	0.047	< .001	[0.165, 0.347]	-0.139	0.113	.220	[-0.361, 0.083]
collect	0.070	0.028	.013	[0.015, 0.126]	0.228	0.046	< .001	[0.138, 0.318]

Note: $^+$: parameter fixed to zero in complete mediation; the standardized solution is STDALL



(a) complete **(b) partial**

Note: Restricted to latent variables. Covariances are not shown for visual clarity. Edges with absolute $\beta < 0.10$ are omitted.

Figure 5: Comparison of complete and partial mediation models

coefficients on both direct and indirect paths, we conclude that a partial mediation is present. Of the privacy concern sub-scales, Control (ctrl) exhibits a total effect of 0.12 with an indirect mediation effect of −0.67. Awareness (aware) yields a total effect of −0.14 with an indirect mediation effect of 0.87. The absolute mediation proportion was 46% in both cases.

D MATERIALS

We include the materials used in the experiments. Table 10 contains the intrinsic manipulations used in the experiments. Table 11 contains the questionnaires used in the study.

Table 10: Content used for intrinsic interventions.

Level	Variant	Content
		Variable: provider
government		At the Government Digital Service our core purpose is to help government work better for everyone in the UK. We do this by building technological services and enforcing digital standards. We value innovation and delivery of user-focused services with the goal of positively impacting individuals, technologies and government.
company		At IBM our core purpose is to promote our client's success. We do this by offering high quality technological and business services in the UK and also around the world. We value intelligence, reason and science with the goal of positively impacting business, society and the human condition.
university^{+}		At [anonymized] University our core purpose is to advance education. We do this through high quality teaching and research [...]. We value academic excellence, innovation and creativity with the goal of positively impacting individuals, organizations and society.
none		[The system] is a new product that lets users give online service providers access to their personal information in a safe and secure way.
		Variable: usage
everyday	Intrinsic	The system gives you the ability to prove personal details to service providers. For instance, you can prove that you are older than the minimum age to buy a product. You can also prove your membership of organizations. You receive a credential on a collection of your personal details which you can then selectively prove to a service provider. You can have multiple identities and can choose which details you wish to disclose. You can verify your identity without revealing details such as your name, nationality and date of birth.
	Presentation	Online providers often require their users to confirm certain information to make sure they eligible for their content. This information can range from phone numbers to home addresses. With [this system], users can choose the information they would like to reveal to service providers. Information that the user does not want the provider to have access to would remain private and protected.
tech^{+}		The system provides its users with a credential. They can use this to prove to service providers that they satisfy the policy to use a service or buy a product. Collaborating with an Issuer organization they receive a credential. The credential is on a set of attributes such as their name, nationality or date of birth. As such, a credential is a digital signature on a list of attribute-value pairs. The user has access to software that takes their credential and provides proof that their attributes fulfill a service provider's policy without revealing the attributes.
		Variable: benefits
user	Intrinsic	Prove your age for media or buying alcohol, without disclosing your date of birth or other data Prove your memberships to gyms, cinemas and universities without being traceable Benefit from your favorite services without the provider being able to profile you
	Presentation	Users are also able to let providers verify their information without giving them direct access to it. This means a user would be able to provide proof to a company that they are over a certain age without telling the company their exact birthdate.
privacy^{+}		Protect privacy by minimizing the data that is disclosed to service providers Enable multiple transactions by a user without these being linkable to each other Transactions can be made with an unlimited number of service providers with a single credential

Note: $^{+}$: Baseline/default condition

Table 11: Adapted questionnaires on perceived trustworthiness and technology acceptance of ACS. All questions are 7-point Likert items, anchored on 1=Strongly Disagree to 7=Strongly Agree. (R) marks reverse-coded items. Questions modified from their original format show the modifications in bold.

Construct	Item	Format	Source
Faith in General Technology [45]: Unmodified			
Faith in Technology (fit)	MKF1	I believe that most technologies are effective at what they are designed to do.	[45]
	MKF2	A large majority of technologies are excellent.	[45]
	MKF3	Most technologies have the features needed for their domain.	[45]
	MKF4	I think most technologies enable me to do what I need to do.	[45]
Trusting Stance (ts)	MKTS1	My typical approach is to trust new technologies until they prove to me that I shouldn't trust them.	[45]
	MKTS2	I usually trust a technology until it gives me a reason not to trust it.	[45]
	MKTS3	I generally give a technology the benefit of the doubt when I first use it.	[45]
Internet users' information privacy concerns (IUIPC) [43]: Unmodified			
Control (ctrl)	ctrl1	Consumer online privacy is really a matter of consumers' right to exercise control and autonomy over decisions about how their information is collected, used, and shared.	[43]
	ctrl2	Consumer control of personal information lies at the heart of consumer privacy.	[43]
	ctrl3	I believe that online privacy is invaded when control is lost or unwillingly reduced as a result of a marketing transaction.	[43]
Awareness (aware)	awa1	Companies seeking information online should disclose the way the data are collected, processed, and used.	[43]
	awa2	A good consumer online privacy policy should have a clear and conspicuous disclosure.	[43]
	awa3	It is very important to me that I am aware and knowledgeable about how my personal information will be used.	[43]
Collection (collect)	coll1	It usually bothers me when online companies ask me for personal information.	[43]
	coll2	When online companies ask me for personal information, I sometimes think twice before providing it.	[43]
	coll3	It bothers me to give personal information to so many online companies.	[43]
	coll4	I'm concerned that online companies are collecting too much personal information about me.	[43]
System Trustworthiness & Acceptance [1]: Refer to "ACS" as object and "privacy" as secondary property.			
Performance Expectancy (perfexp) ⟺ Primary Usefulness (primuse)	STPE1	I **would** find **anonymous credential systems** useful in my daily life.	[1]
	STPE2	Using **anonymous credential systems** increases my chances of achieving tasks that are important to me.	[1]
	STPE3	Using **anonymous credential systems** helps me accomplish tasks more quickly.	[1]
	STPE4	Using **anonymous credential systems** increases my productivity.	[1]
Effort Expectancy (effexp) ⟺ Ease of Use (ease)	STEE1	Learning how to use **anonymous credential systems** is easy for me.	[1]
	STEE2	My interaction with **anonymous credential systems** is clear and understandable.	[1]
	STEE3	I find **anonymous credential systems** easy to use.	[1]
	STEE4	It is easy for me to become skilful at using **anonymous credential systems**.	[1]
Facilitating Conditions (fc)	STFC1	I have the resources necessary to use **anonymous credential systems**.	[1]

Construct	Item	Format	Source
	STFC2	I have the knowledge necessary to use **anonymous credential systems**.	[1]
	STFC3	**Anonymous credential systems are** compatible with other technologies I use.	[1]
	STFC4	I can get help from others when I have difficulties using **anonymous credential systems**.	[1]
Behvarioral Intention (bi)	STBI1	I intend to use **anonymous credential systems** in the future.	[1]
	STBI2	I will always try to use **anonymous credential systems** in my daily life.	[1]
	STBI3	I plan to use **anonymous credential systems** in future.	[1]
	STBI4	I predict I would use **anonymous credential systems** in the future.	[1]
Perceived Trustworthiness (trust)	STT1	I believe that **anonymous credential systems** are trustworthy.	[1]
	STT2	I trust in **anonymous credential systems**.	[1]
	STT3	I do not doubt the honesty of **anonymous credential systems**.	[1]
	STT4	I feel assured that legal and technological structures adequately protect me from problems on **anonymous credential systems**.	[1]
	STT5	Even if not monitored, I would trust **anonymous credential systems** to do the job right.	[1]
	STT6	**Anonymous credential systems** have the ability to fulfil their task.	[1]
Technology Acceptance Model (TAM 2.0) [57]: Refer to "ACS" as object and "privacy" as secondary property.			
Perceived Usefulness (useful) ⟺ Secondary Usefulness ⟺ Privacy Usefulness (privuse)	TAU1	Using the system improves my **ability to do what I need to in terms of privacy protection**.	[57]
	TAU2	Using the system in my **day to day life increases my privacy protection**.	[57]
	TAU3	Using the system enhances the **privacy of my personal information**.	[57]
	TAU4	I find the system to useful to **complete tasks requiring privacy protection**.	[57]
Perceived Ease of Use (ease)	TAE1	My interaction with the system is clear and understandable.	[57]
	TAE2	Interacting with the system does not require a lot of my mental effort.	[57]
	TAE3	I find it easy to get the system to do what I want it to do.	[57]
	TAE4	I find the system to be easy to use.	[57]
Results Demonstrability (results)	TAR1	I have no difficulty telling others about the results of using the system.	[57]
	TAR2	I believe I could communicate to others the consequences of using the system.	[57]
	TAR3	The results of using the system are apparent to me.	[57]
	~~rTAR4~~	~~I would have difficulty explaining why using the system may or may not be beneficial.~~ (**R**) [Removed due to inconsistency with sub-scale.]	[57]
Not included in the final model			
System Trustworthiness & Acceptance [1]: Refer to "ACS" as object and "privacy" as secondary property.			
Social Influence (si)	STSI1	People who are important to me think that I should use **a system, such as an anonymous credential system, to protect my privacy**.	[1]
	STSI2	People who influence my behaviour think that I should use **a system, such as an anonymous credential system, to protect my privacy**.	[1]
	STSI3	People whose opinions that I value prefer that I use **a system, such as an anonymous credential system, to protect my privacy**.	[1]
Trustworthiness Provider [10]: Refer to subject as "user"			
Ability (ability)	TPA1	This provider is very competent.	[10]
	TPA2	This provider is able to fully satisfy its **users**.	[10]
	TPA3	One can expect good advice from this provider.	[10]
Benevolence (benevol)	TPB1	This provider is genuinely interested in its **users'** welfare.	[10]

Construct	Item	Format	Source
	TPB2	This provider puts **users'** interests first.	[10]
	TPB3	If problems arise, one can expect to be treated fairly by this provider.	[10]
Integrity (integrity)	TPI1	I am happy with the standards by which this provider is operating.	[10]
	TPI2	This provider operates scrupulously.	[10]
	TPI3	You can believe the statements of this provider.	[10]
Predictability (predict)	rTPP1	This provider's methods of operation are unclear. (**R**)	[10]
	TPP2	This provider keeps its promises.	[10]
	TPP3	I would rely on advice from this provider.	[10]
Alternative System Trustworthiness [19]: Refer to object "Website" as ACS			
Honesty (honest)	STCH1	The **anonymous credential system** provides truthful information.	[19]
	STCH2	The **anonymous credential system** is believable.	[19]
	STCH3	The features of the **anonymous credential system** reflect expertise.	[19]
Reputation (rep)	STCRe1	The **anonymous credential system** is respected.	[19]
	STCRe2	The **anonymous credential system** has a good reputation.	[19]
Risk (risk)	STCR1	I am taking a chance interacting with this **anonymous credential system**.	[19]
	STCR2	I feel that it is unsafe to interact with this **anonymous credential system**.	[19]
	STCR3	I feel I must be cautious when using this **anonymous credential system**.	[19]
	STCR4	It is risky to interact with this **anonymous credential system**.	[19]
Trusting Belief Reliability [45]: Refer to object ACS			
Reliability (reliable)	TB1	The **anonymous credential system** is a very reliable piece of software.	[45]
	TB2	The **anonymous credential system** does not fail me.	[45]
	TB3	The **anonymous credential system** is extremely dependable.	[45]
	TB4	The **anonymous credential system** does not malfunction for me.	[45]