A Privacy Calculus Model for Contact Tracing Apps: Analyzing the German Corona-Warn-App

David Harborth[0000−0001−9554−7567] and Sebastian Pape[0000−0002−0893−7856]

Chair of Mobile Business and Multilateral Security
Goethe University, Frankfurt, Germany

Abstract. The SARS-CoV-2 pandemic is a pressing societal issue today. The German government promotes a contract tracing app named Corona-Warn-App (CWA), aiming to change citizens' health behavior during the pandemic by raising awareness about potential infections and enable infection chain tracking. Technical implementations, citizens' perceptions, and public debates around apps differ between countries, i.e., in Germany there has been a huge discussion on potential privacy issues of the app. Thus, we analyze effects of privacy concerns regarding the CWA, perceived CWA benefits, and trust in the German healthcare system to answer why citizens use the CWA. We use a sample with 1,752 actual users and non-users and find support for the privacy calculus theory, i. e., individuals weigh privacy concerns and benefits in their use decision. Thus, citizens' privacy perceptions about health technologies (e. g., shaped by public debates) are crucial as they can hinder adoption and negatively affect future fights against pandemics.

Keywords: Covid-19 · Contact tracing apps · Information privacy

1 Introduction

With the global pandemic caused by the severe acute respiratory syndrome coronavirus 2 (SARS-CoV-2), digital proximity tracing systems to identify people who have been in contact with an infected person became a hot topic. Technical implementations, citizens' perceptions, and public debates around apps differ between countries, especially because of differences in the perceived importance of data protection. In particular in Germany, there have been many discussions on different implementations and their architecture [15], i. e. if the approach should be centralized or decentralized. As a result, the German contract tracing app named Corona-Warn-App (CWA) was build with a strong focus on privacy. It is based on the DP-3T protocol which ensures data minimization, prevents abuse of data and the tracking of users [14]. The German government along with its associated health institutes promote the use of the CWA, aiming to change citizens' health behavior during the pandemic by raising awareness about potential infections and enable effective infection chain tracking.

While the discussion on the architecture and possible effects of it was mostly among experts, for a widespread use of the app, the app's acceptance by ordinary persons is of more importance [55]. Privacy concerns have been identified as one of the major barriers for the acceptance of contact tracing apps in prior work [30, 4]. The privacy calculus theory, in which individuals make their use decision by weighing privacy concerns and benefits is a suitable framework to explain the citizens' health behavior related to using the CWA [12, 16, 41, 56, 18, 19, 28]. The citizens' decision is of even more importance in countries like Germany where the use of the contact tracing app is voluntary and not enforced by the government. To the best of our knowledge, previous studies on contact tracing apps facilitating the privacy calculus are based on users' intentions rather than on their behavior. Therefore, we investigate the factors influencing the actual CWA use decisions on an individual level with a sample of 1,752 participants (896 CWA users / 856 non-users) and address the question why citizens use contact tracing apps.

2 Privacy-Related Decision Making and Tracing Apps

The privacy-related decision making process of users is explained by several approaches and constructs in prior work [53, 40, 44, 52]. The privacy calculus is one of the approaches aiming at explaining the role of privacy concerns in use behaviors, such as information disclosure or technology use. It represents a deliberate trade-off made by individuals weighing up benefits and costs [37, 9, 12]. The calculus assumes that if benefits outweigh the risks (i. e., privacy concerns [12]) users tend to engage in the privacy-related behavior. Empirical studies find that privacy risks negatively influence use intentions or behaviors and benefits positively influence the outcome variables [36, 23]. The deliberate privacy-related decision making by users is questioned in more recent studies, e. g., by extending the original concepts of the privacy calculus with new factors [34, 10] or by introducing behavioral biases influencing the trade-off [13, 24].

Naturally, recent research on Covid-19 apps is sprouting up everywhere. A huge part consists of surveys on the users' adoption of one or more contact tracing apps, e. g. in Australia [16], China [35], France [1], Germany [35, 1, 4, 45, 47, 41, 56], Ireland [46, 18], Italy [1], Switzerland [4, 56], Taiwan [19], the UK [1, 31, 39], and the US [35, 1, 28]. For example, Horstmann et al. found for a sample in Germany that the most common reasons for non-users were privacy concerns, lack of technical equipment, and doubts about the app's effectiveness [30]. Most of the other studies had similar results and identified privacy concerns as the or one of the main barriers to use contact tracing apps. In particular, people worried about corporate or government surveillance, potentially even after the pandemic [46], leakage of data to third parties [1], exposure of social interactions [4], and secondary use of the provided data [4]. However, misconceptions based on widespread knowledge gaps accompany the adoption of contract tracing apps [47].

Several of the mentioned studies on COVID-19 contact tracing apps have used the privacy calculus [16, 41, 4, 18, 19, 28]. Some of them combined the privacy calculus with other constructs such as technology acceptance [16], social influence [16, 18], or herding effects [56]. All studies found significant effects from benefits and privacy concerns on use intentions. However, all of them used self-reported download, install, and (continuous) use intentions as dependent variables. In contrast, our model relies on a quasi-observable factor (use of the CWA or not) which results from sampling participants, thereby, decreasing biases such as the social desirability bias. Furthermore, we refer to trust in the German healthcare system in contrast to trust in app developers [41] or service providers [39] since Horvath et al. found that users' trust in publicly-funded institutions, i.e., the British National Health Service can reduce privacy concerns [31]. For the sake of our cross-sectional online survey, we fall back on the original concepts of the privacy calculus – risks, benefits and CWA use – and nest it within the nomological net of the original "antecedents–privacy concerns–outcomes model" (APCO) [52]. We discuss the emerging research model and hypotheses in the next section.

3 Method

We present our questionnaire, data collection and research model in this section. We used the statistical software R (version 4.0.3) for the descriptive analyses and SmartPLS (version 3.3.2) [50] for the structural equation modeling.

3.1 Questionnaire and Data Collection

We adapted the constructs for privacy concerns (PC) and perceived benefits (PB) from prior literature [20, 5] and applied it to the CWA. Trust in the German healthcare system is based on the construct by Pavlou [48]. The use of the CWA is measured with a binary variable indicating whether participants use the CWA (Use=1) or not (Use=0). We conducted the study with a certified panel provider in Germany (ISO 20252 norm). The survey was implemented with LimeSurvey (version 2.72.6) [51] and hosted on a university server. We sampled the participants in a way to achieve a representative sample for Germany with approximately 50% females and 50% males as well as an age distribution following the EUROSTAT2018 census [17]. We also set a quota to end up with half of the sample using the CWA and the other half not using it. Our resulting sample consists of 1752 participants which is representative for Germany with respect to age and gender. The same diversity can be observed for income and education (see Tab. 1). 896 participants use the CWA (51.14%) and 856 do not (48.86%). 1299 use Android (74.14%), 436 use iOS (24.89%) and 17 stated to use smartphones with other mobile operating systems (OS) (0.97%).

Since we divided the sample into two approximately equal groups (CWA users and non-users), we check for statistically significant differences in the demographics between the groups. This is required to rule out confounding influences of these variables. All variables are non-normally distributed (based on Shapiro-Wilk tests for normality). Thus, we conducted Wilcoxon rank-sum tests to assess possible differences between CWA users and non-users.

Age and gender show no statistically significant differences since due to our sampling strategy. There are statistically significant differences between users and non-users of the CWA for the remaining demographics. Income is

Table 1: Participants' characteristics for age, gender, income and education

Demographics	N	%
Age		
18-29 years	371	21.17%
30-39 years	316	18.04%
40-49 years	329	18.78%
50-59 years	431	24.60%
60 years and older	305	17.41%
Net income		
500€- 1000€	160	9.13%
1000€- 2000€	402	22.95%
2000€- 3000€	404	23.06%
3000€- 4000€	314	17.92%
More than 4000€	292	16.67%
Prefer not to say	180	10.27%

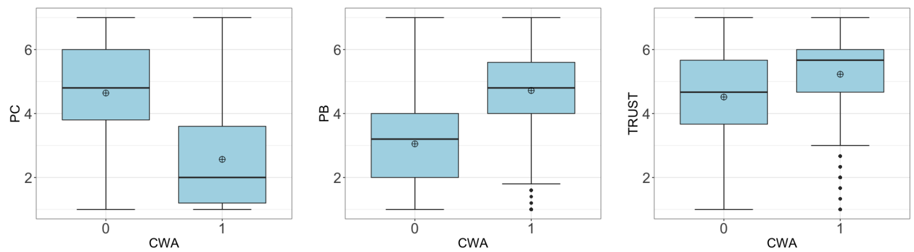
Demographics		N	%
Gender			
	Female	894	51.03%
	Males	853	48.69%
	Diverse	4	0.23%
	Prefer not to say	1	0.06%
Education			
1	No degree	8	0.46%
2	Secondary school	187	10.67%
3	Secondary school+	574	32.76%
4	A levels	430	24.54%
5	Bachelor's degree	240	13.70%
6	Master's degree	285	16.27%
7	Doctorate	28	1.60%

+5 GCSEs at grade C and above

significantly higher for users compared to the non-users. However, the median is the same which is why we argue that the absolute difference is not having a substantial confounding effect on our analysis. The same argumentation holds for education with a median of 4 for users and 3.5 for non-users, smartphone experience in years with a mean 8.77 for users and 8.35 for non-users as well as experience in years with the respective smartphone OS (mean 7.85 for users and 7.46 for non-users). The used smartphone OS by participants in both groups is roughly similar with significantly more Android users in both groups (about three times more Android users compared to iOS). This distribution of operating systems is representative for Germany [54]. Thus, all differences between groups are – although statistically significant – negligible for our analysis since the absolute differences are relatively small. We also calculated mean sum scores for privacy concerns, perceived benefits and trust in the German healthcare system in order to check for differences between CWA users and non-users. We conducted Shapiro-Wilk tests for normality and Levene's tests of equal variances for the three constructs and find that they are not normally distributed and do not have equal variances between CWA users and non-users. Due to the non-parametric properties of our data we used the Wilcoxon rank-sum test. All variables are statistically significantly different between users and non-users with large to moderate effect sizes r for privacy concerns (r=-0.540, cf. Figure 1a), perceived benefits (r=-0.553, cf. Figure 1b), and trust (r=-0.258, cf. Figure 1c).

3.2 Research Model and Hypotheses

We operationalize the "antecedents - privacy concerns - outcome" (APCO) model on an individual level, i. e., excluding factors such as cultural or organizational



(a) Privacy Concerns (b) Perceived Benefits (c) Trust Healthcare System

Fig. 1: Boxplots for Privacy Concerns, Perceived Benefits and Trust in the German Healthcare System

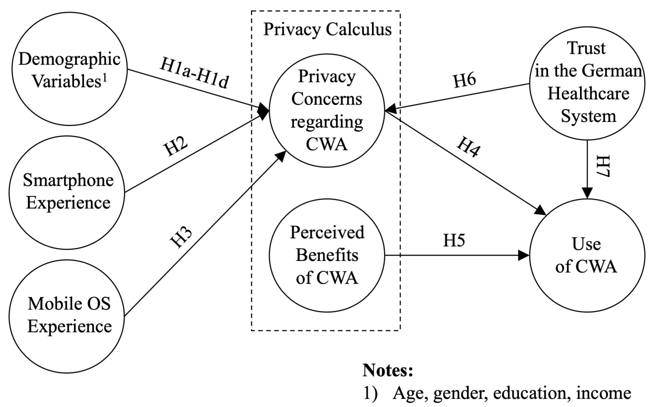


Fig. 2: Research Model

ones [52]. We focus on a narrow set of common antecedents on an individual level which are relevant for the case of the Corona-Warn-App. Privacy concerns are operationalized contextually, i. e. focusing on the specific perceptions of individuals related to the CWA. The outcome is the CWA use explained by the privacy calculus including trust in the German healthcare system as an additional antecedent of privacy concerns. Thus, this nomological net is mostly based on the original APCO model [52]. The resulting research model is shown in Figure 2.

We include four demographic variables as antecedents (age, gender, income, education). The results for the effects of these antecedents in previous studies are inconclusive [25]. Prior work finds that older individuals and women are more concerned about their privacy [32, 57]. We follow these findings and hypothesize that age has a positive effect on privacy concerns regarding the CWA and that females show higher levels of privacy concerns. Higher levels of education are usually associated with increasing privacy concerns [38]. However, since the German CWA was build based on privacy by design and can be considered to be privacy friendly, a better understanding of the CWA should reduce privacy concerns [47]. Thus, we hypothesize that there is a negative effect of education on privacy concerns (i. e., higher education levels correspond to lower privacy concerns). Similarly, a higher income is hypothesized to have a negative effect on privacy concerns as well (i. e., higher income levels correspond to lower privacy concerns) [52]. We hypothesize for the demographic variables:

1. (a) *Age has a positive effect on privacy concerns regarding the CWA.*
   (b) *Female participants show higher levels of privacy concerns regarding the CWA.*
   (c) *Education has a negative effect on privacy concerns regarding the CWA.*
   (d) *Income has a negative effect on privacy concerns regarding the CWA.*

Smartphone experience and the experience with the respective mobile operating system is included as control for participants technical experience by including these variables as antecedents of privacy concerns [26]. We argue that participants with more experience regarding both dimensions have higher privacy concerns as they might have witnessed more privacy-related breaches and attacks on smartphones [3, 11]. Thus, we hypothesize:

2. *Smartphone experience has a positive effect on privacy concerns regarding the CWA.*
3. *Experience with the mobile OS has a positive effect on privacy concerns regarding the CWA.*

Individuals' privacy concerns are generally assumed to have a negative effect on the outcome variables [52]. In contrast to prior work on the CWA and privacy, we use the actual use decisions of participants instead of behavioral intentions. By that, we avoid biases in our results due to the behavioral-intention gap which is especially pronounced in privacy-related research [8]. Thus, we hypothesize:

4. *Privacy concerns regarding the CWA have a negative effect on the decision to use the app.*

Prior work finds that the relation between privacy concerns and behavior is also affected by other factors. The most common rationale is the privacy calculus which is also included in the APCO model. The privacy calculus states that individuals engage in a deliberate trade-off between benefits (of using a technology or disclosing information) and costs (privacy risks which are operationalized by privacy concerns) when making privacy-related decisions [12]. To account for this trade-off, we include the perceived benefits of using the CWA and hypothesize:

5. *The perceived benefits of using the CWA have a positive effect on the decision to use the app.*

Our last variable in the model is trust in the German healthcare system. We include this variable as trust in general is an important concept to explain privacy concerns and individual behavior [52]. In general, trust in certain entities alleviates privacy concerns related to these entities. In addition, trust has a direct positive effect on certain use or disclosure behaviors [40, 23, 27, 33]. In the context of the pandemic and contact tracing apps, it can be seen that privacy concerns can be alleviated by users' trust in certain publicly-funded institutions, such as the British National Health Service (NHS) [31]. Our construct covers this partially as we include a more abstract notion of this idea in our model.

6. *Trust in the German healthcare system has a negative effect on the privacy concerns regarding the CWA.*
7. *Trust in the German healthcare system has a positive effect on the decision to use the app.*

4 Results

An analysis of the measurement model regarding reliability and validity is a precondition for interpreting the results of the structural model [22]. For the PLS algorithm, we chose the path weighting scheme with a maximum of 300 iterations and a stop criterion of 10^{-7}. For the bootstrapping procedure, we used 5000 bootstrap subsamples and no sign changes as the method for handling sign changes during the iterations of the bootstrapping procedure.

4.1 Assessment of the Measurement Model

Internal Consistency Reliability Internal consistency reliability (ICR) measurements indicate how well certain indicators of a construct measure the same latent phenomenon. Two standard approaches for assessing ICR are Cronbach's α and the composite reliability. The values of both measures should be between 0.7 and 0.95 for research that builds upon accepted models [21]. Values for Cronbach's α (0.896, 0.960 and 0.867) and composite reliability (0.903, 0.965 and 0.895) for perceived benefits (PB), privacy concerns (PC) and trust in the healthcare system (TRUST), respectively, are within these suggested ranges.

Convergent Validity We evaluate convergent validity based on the outer loadings of the indicators of the constructs (indicator reliability) and the average variance extracted (AVE) [22]. The lowest loading of the three constructs equals 0.796. Thus, indicator reliability is established as loadings above 0.7 imply that the indicators have much in common, which is desirable for reflective measurement models [21]. Convergent validity for the construct is assessed by the AVE (sum of the squared loadings divided by the number of indicators). The AVEs are 0.706 for PB, 0.864 for PC, and 0.790 for TRUST. This indicates that the constructs explain significantly more than half of the variance of the indicators, and thereby demonstrates convergent validity.

Discriminant Validity We assess the degree of uniqueness of a construct compared to other constructs by investigating the cross-loadings for the single indicators. All outer loadings of a certain construct should be larger than its cross-loadings with other constructs [22] which is the case for our model. On a construct level, we compare the square root of the constructs' AVE with the correlations with other

Table 2: Heterotrait-Monotrait Ratio (HTMT)

	AGE	EDU	GDR	INCOME	Sp. Exp.	MOS Exp.	PB	PC	USE
EDU	0.152								
GDR	0.012	0.045							
INCOME	0.048	0.243	0.088						
Smartphone Exp.	0.148	0.052	0.044	0.123					
Mobile OS Exp.	0.008	0.002	0.067	0.113	0.676				
Perc. Benefits	0.045	0.057	0.051	0.043	0.025	0.018			
Privacy Concerns	0.040	0.155	0.035	0.096	0.020	0.027	0.502		
USE	0.017	0.151	0.014	0.139	0.078	0.067	0.574	0.554	
TRUST	0.064	0.136	0.042	0.068	0.028	0.031	0.481	0.425	0.281

constructs. The square root of the AVE of a single construct should be larger than the correlation with other constructs (Fornell-Larcker criterion) [21]. All values are larger than correlations with other constructs, indicating discriminant validity. Prior work proposes the heterotrait-monotrait ratio (HTMT) as a superior approach for assessing discriminant validity [29]. Values close to 1 for HTMT indicate a lack of discriminant validity. A conservative threshold is 0.85 [29] and no value in our model is above the suggested threshold of 0.85 (Table 2). We assess if the HTMT statistics are significantly different from 1 with a bootstrapping procedure with 5,000 subsamples to get the confidence interval in which the true HTMT value lies with a 95% chance. The HTMT measure requires that no confidence interval contains the value 1. Our analysis shows that this is the case. Thus, discriminant validity is established.

Common Method Bias The common method bias (CMB) can occur if data is gathered with a self-reported survey at one point in time in one questionnaire [49]. We need to test for the CMB since this is the case in our study. We perform a principal component factor analysis in R to conduct the Harman's single-factor test to address the issue of CMB [49]. The assumptions of the test are that CMB is not an issue if there is no single factor that results from the factor analysis or that the first factor does not account for the majority of the total variance [49]. The test shows that six factors have eigenvalues larger than 1 which account for 75.72% of the total variance. The first factor explains 34.65% of the total variance. Thus, we argue that CMB is not likely to be an issue in the data set.

4.2 Structural Model Assessment and Results

We assess collinearity, the level of R^2, the path coefficients, the effect size f^2, the predictive relevance Q^2, and the effect size q^2. We address these evaluation steps to ensure the predictive power of the model with regard to the target constructs privacy concerns and use.

Collinearity Collinearity is present if two predictor variables are highly correlated with each other. To address this issue, we assess the inner variance inflation factor (VIF). All VIFs above 5 indicate that collinearity between constructs is present. For our model, the highest VIF is 1.939. Thus, collinearity is not an issue.

Table 3: Path Estimates and Effect Sizes f^2 and q^2 (only at least small effects sizes f^2 and q^2 shown)

	Relation	Path Estimate	f^2	q^2	Result
H1a	Age → Privacy Concerns	-0.039			Not conf.
H1b	Gender → Privacy Concerns	-0.017			Not conf.
H1c	Education → Privacy Concerns	-0.097^{***}			Confirmed
H1d	Income → Privacy Concerns	-0.045^{*}			Confirmed
H2	Smartphone Exp. → Privacy Concerns	-0.050			Not conf.
H3	Mobile OS Exp. → Privacy Concerns	0.055			Not conf.
H4	Privacy Concerns → Use of CWA	-0.378^{***}	0.177	0.149	Confirmed
H5	Perceived Benefits → Use of CWA	0.395^{***}	0.185	0.181	Confirmed
H6	Trust in the German Healthcare System → Privacy Concerns	-0.374^{***}	0.164	0.137	Confirmed
H7	Trust in the German Healthcare System → Use of CWA	-0.054^{*}			Rejected

Significance and Relevance of Model Relationships Values of adjusted R^2 are equal to 16.6% and 40.7% for privacy concerns and use, respectively. These values can be interpreted as as weak and moderate for privacy concerns and use of the CWA [22]. The path estimates for our research model (see Figure 2) are shown in Table 3. The sizes of significant path estimates are interpreted relative to each other in the model. Based on this, the effects of privacy concerns and perceived benefits on the use of the CWA (confirming H4 and H5) as well as of trust in the German healthcare system on privacy concerns (confirming H6) are strong. Education and income have statistically significant weak negative effects on privacy concerns (confirming H1c and H1d). However, both effect sizes are so small that they cannot be considered as relevant in the model (also visible in the f^2 effect sizes which are lower than the lowest suggested threshold of 0.02 [7]). Trust in the German healthcare system has a weak but negative effect on the use of the CWA (rejecting H7). None of the other hypotheses are significant.

Effect Sizes f^2 The f^2 effect size measures the impact of a construct on the endogenous variable by omitting it from the analysis and assessing the resulting change in the R^2 value [21]. The values are assessed based on thresholds by Cohen [7], who defines effects as small, medium and large for values of 0.02, 0.15 and 0.35, respectively. The effect sizes f^2 correspond to the path estimates with medium-sized effects of privacy concerns and perceived benefits on use of the CWA and trust in the healthcare system on privacy concerns (Table 3).

Predictive Relevance Q^2 The Q^2 measure indicates the out-of-sample predictive relevance of the structural model with regard to the endogenous latent variables based on a blindfolding procedure [21]. We used an omission distance d=7 with recommended values between five and ten [22]. Furthermore, we report the Q^2 values of the construct cross-validated redundancy approach, since this approach is based on both the results of the measurement model as well as of the structural model [21]. Detailed information about the calculation cannot be provided due to space limitations. For further information see Chin [6]. Values above 0 indicate that the model has the property of predictive relevance. In our case, the Q^2 value is equal to 0.145 for PC and 0.404 for use. Since they are larger than zero, predictive relevance of the model is established.

Effect Sizes q^2 The assessment of q^2 follows the same logic as the one of f^2. It is based on the Q^2 values of the endogenous variables and calculates the individual predictive power of the exogenous variables by omitting them and comparing the change in Q^2 [21]. All individual values for q^2 are calculated with an omission distance d of seven. The thresholds for the f^2 interpretation can be applied, too [7]. The results show that the individual predictive power for hypotheses 4, 5 and 6 is given with medium-sized effects.

5 Discussion

We investigated the impact of privacy concerns related to the CWA, benefits of the CWA and trust in the German healthcare system on the CWA use decision. We used the APCO model [52] and the privacy calculus theory [12] for the hypothesis development and evaluated them with an online survey with 1,752 participants in Germany (896 users and 856 non-users).

Our results support the privacy calculus theory and that individuals weigh up risks and benefits as privacy concerns have a statistically significant negative effect and benefits have a statistically significant positive effect on use. We also find that trust in the German healthcare system is the important antecedent of privacy concerns by alleviating them. This confirms our hypothesis and indicates that participants associate trust in the healthcare system with the entities operating the CWA (Robert Koch Institute, part of the healthcare system as it is subordinated to the German Federal Ministry of Health). In this context, is it far more interesting that the direct positive effect of trust on the use cannot be found in the data. The effect is even negative (although the effect size is negligible). The hypotheses related to the antecedents education and income can be accepted, although the effect size for both effects is relatively small.

Related work on contact tracing app adoption in Germany based on the privacy calculus uses a different set of antecedents of privacy concerns, referred to trust to the app designers and the study used intentions to use the app as a target variable [41]. However, as in our work, they find statistically significant effects of benefits (positive) and concerns (negative) on intentions. Furthermore, trust has a negative effect on privacy concerns and a positive effect on intentions. Thus, our study with actual use decisions as dependent variable confirms that the privacy calculus is an appropriate tool to explain the CWA use.

5.1 Limitations

Our work has the following limitations. First, our study covers only the German Corona-Warn-App with all the respective characteristics of this app. Thus, the results are only generalizable to contact tracing apps in other countries to the extent that the population is comparable to the German population and that comparable apps have similar characteristics related to privacy and security aspects. However, even if apps in other countries are technically comparable, other influencing factors such as a positive or negative media coverage, failures in implementation efforts, etc., could still lead to different evaluations of individuals. Second, although we could minimize the effect of biases due to the study design (online questionnaire, self-reported measures) by having an observable dependent variable instead of reported use behaviors or intentions, we still had to rely on self-reported measures for the constructs in our model. Furthermore, our analysis closely followed the original APCO model with its focus on privacy concerns [52]. Thus, we did not consider interactions between antecedents or other potential relationships between other variables of the calculus such as effects of demographics on the perceived benefits of the CWA.

5.2 Future Work

The previously described effects could be considered in future work. For example, there were reports that more wealthy households were less affected by the pandemic not only from an economically but also in their daily lives, e.g., by having access to private transportation and enough living space [42]. We would assume that income has a negative effect on the perceived benefits as these households do not profit as much from technical solutions like the CWA. Similarly, the effect of trust in the healthcare system on use decisions could also be mediated by perceived benefits of the app as participants with higher trust in the medical care could be less cautious and do not see the benefits of such apps.

Besides interesting opportunities in extending the model and consider that there could be antecedents for the other variables in the APCO model and privacy calculus, we see the need for analyses of privacy and health behavior apps across countries alongside with analyses of causes for differences in potential privacy perceptions. Furthermore, it would be interesting to investigate to what extent contact tracing apps such as the CWA could induce a change in the health-related behaviors of individuals, e.g., did a notification about a past risk contact change the consequent behavior of individuals by making them more cautious?

Closely related is the question how individuals are influenced by politicians, the public debate, and others in their decision to adopt technologies like the CWA. We argued that these social influences could have been a major driver for the division of the German population into a group which does not believe that there are benefits of such apps and that privacy issues are too severe and into the group which uses the app. Thus, future work could analyze the influences in a more granular way in order to assess the reasons for this division. This is especially important since it has been shown that informative and motivational video messages have very limited effect, but even small monetary incentives can increase the app's adoption [43]. Thus, besides improving the citizens' knowledge and perception of privacy mechanisms and benefits of the app, future health behavior communication could make use of small monetary incentives, promote the app's benefits or even try to nudge citizens to use the app.

6 Conclusion

In summary, our work contributes to the current work on contact tracing apps in two ways. First, we provide – to the best of our knowledge – one of the first research findings which rely on an observable outcome variable measuring the actual contact tracing app use decisions of German citizens in a large-scale online survey; thus, avoiding certain biases (e.g., the intention-behavior gap [8]) and providing robust results to rely on for deriving practical recommendations.

Second, we practically recommend to consider the importance of appropriate communication strategies by policy makers when releasing health behavior apps, such as the CWA, to a large heterogeneous user base, especially when faced with crises such as a pandemics. We can see high levels of privacy concerns and significantly lower levels of perceived benefits in the group of non-users. In contrast, trust in the healthcare system is almost equal between groups. One possible explanation is that even though the CWA is developed in a privacy-friendly way politicians and media failed to properly explain the app's functions and data protection measures (e. g., decentralized approach) to the German citizens, and by that lost several millions of potential users. This is supported by a study on media coverage which found that governments or politicians were criticized for their lack of transparent communication [2]. In addition, the public debate around the German CWA was rather critical and the usefulness of the app was questioned on a daily basis [15, 55]. This implies that there was no real strategy on how to introduce the app to the citizens and advocate it against expectable criticism which needs to be considered in future crises.

Acknowledgements

This work was supported by the Goethe-Corona-Fonds from Goethe University Frankfurt and the European Union's Horizon 2020 research and innovation program under grant agreement 830929 (CyberSecurity4Europe).

References

1. Altmann, S., Milsom, L., Zillessen, H., Blasone, R., Gerdon, F., Bach, R., Kreuter, F., Nosenzo, D., Toussaert, S., Abeler, J.: Acceptability of app-based contact tracing for covid-19: Cross-country survey evidence (2020)
2. Amann, J., Sleigh, J., Vayena, E.: Digital contact-tracing during the covid-19 pandemic: an analysis of newspaper coverage in germany, austria, and switzerland. Plos one **16**(2), e0246524 (2021)
3. Bellman, S., Johnson, E.J., Kobrin, S.J., Lohse, G.L.: International differences in information privacy concerns: A global survey of consumers. The Information Society **20**(5), 313–324 (2004)
4. Bonner, M., Naous, D., Legner, C., Wagner, J.: The (lacking) user adoption of covid-19 contact tracing apps–insights from switzerland and germany. In: Proceedings of the 15th Pre-ICIS Workshop on Information Security and Privacy. vol. 1 (2020)

5. Champion, V.L.: Instrument development for health belief model constructs. Advances in nursing science (1984). https://doi.org/10.1097/00012272-198404000-00011
6. Chin, W.W.: The Partial Least Squares Approach to Structural Equation Modeling. In: Marcoulides, G.A. (ed.) Modern Methods for Business Research, pp. 295–336. Lawrence Erlbaum, Mahwah, NJ (1998)
7. Cohen, J.: Statistical Power Analysis for the Behavioral Sciences. HillsDale, NJ (1988)
8. Crossler, R.E., Johnston, A.C., Lowry, P.B., Hu, Q., Warkentin, M., Baskerville, R.: Future directions for behavioral information security research. Computers and Security **32**(June), 90–101 (2013)
9. Culnan, M.J., Armstrong, P.K.: Information Privacy Concerns, Procedural Fairness, and Impersonal Trust: An Empirical Investigation. Organization Science **10**(1), 104–115 (feb 1999). https://doi.org/10.1287/orsc.10.1.104, `http://pubsonline.informs.org/doi/abs/10.1287/orsc.10.1.104`
10. Dienlin, T., Metzger, M.J.: An Extended Privacy Calculus Model for SNSs: Analyzing Self-Disclosure and Self-Withdrawal in a Representative U.S. Sample. Journal of Computer-Mediated Communication **21**(5), 368–383 (2016). https://doi.org/10.1111/jcc4.12163
11. Dinev, T., Hart, P.: Internet privacy concerns and social awareness as determinants of intention to transact. International Journal of Electronic Commerce **10**(2), 7–29 (2005)
12. Dinev, T., Hart, P.: An extended privacy calculus model for e-commerce transactions. Information Systems Research **17**(1), 61–80 (2006). https://doi.org/10.1287/isre.1060.0080
13. Dinev, T., Mcconnell, A.R., Smith, H.J.: Informing Privacy Research Through Information Systems, Psychology, and Behavioral Economics: Thinking Outside the "APCO" Box. Information Systems Research **26**(4), 639–655 (2015)
14. DP-3T Project: Decentralized privacy-preserving proximity tracing (2020), `https://github.com/DP-3T/documents/blob/master/DP3T%20White%20Paper.pdf`
15. DP-3T Project: Privacy and security risk evaluation of digital proximity tracing systems (2020), `https://github.com/DP-3T/documents/blob/master/Security%20analysis/Privacy%20and%20Security%20Attacks%20on%20Digital%20Proximity%20Tracing%20Systems.pdf`
16. Duan, S.X., Deng, H.: Hybrid analysis for understanding contact tracing apps adoption. Industrial Management & Data Systems (2021)
17. EUROSTAT: EUROSTAT 2018. `https://ec.europa.eu/eurostat/de/home` (2021)
18. Fox, G., Clohessy, T., van der Werff, L., Rosati, P., Lynn, T.: Exploring the competing influences of privacy concerns and positive beliefs on citizen acceptance of contact tracing mobile applications. Computers in Human Behavior **121**, 106806 (2021)
19. Garrett, P.M., Wang, Y., White, J.P., Hsieh, S., Strong, C., Lee, Y.C., Lewandowsky, S., Dennis, S., Yang, C.T.: Young adults view smartphone tracking technologies for covid-19 as acceptable: the case of taiwan. International journal of environmental research and public health **18**(3), 1332 (2021)
20. Gu, J., Xu, Y.C., Xu, H., Zhang, C., Ling, H.: Privacy concerns for mobile app download: An elaboration likelihood model perspective. Decision Support Systems **94**, 19–28 (2017). https://doi.org/10.1016/j.dss.2016.10.002
21. Hair, J., Hult, G.T.M., Ringle, C.M., Sarstedt, M.: A Primer on Partial Least Squares Structural Equation Modeling (PLS-SEM). SAGE Publications (2017)

22. Hair, J., Ringle, C.M., Sarstedt, M.: PLS-SEM: Indeed a Silver Bullet. Journal of Marketing Theory and Practice **19**(2), 139–152 (2011)
23. Harborth, D., Pape, S.: Investigating Privacy Concerns related to Mobile Augmented Reality Applications. In: International Conference on Information Systems (ICIS). pp. 1–9 (2019)
24. Harborth, D., Pape, S.: Empirically Investigating Extraneous Influences on the "APCO" Model – Childhood Brand Nostalgia and the Positivity Bias. Future Internet **12**(12), 1–16 (2020). https://doi.org/10.3390/fi12120220
25. Harborth, D., Pape, S.: Empirically Investigating Extraneous Influences on the "APCO" Model—Childhood Brand Nostalgia and the Positivity Bias. Future Internet **12**(12), 220 (dec 2020). https://doi.org/10.3390/fi12120220, `https://www.mdpi.com/1999-5903/12/12/220`
26. Harborth, D., Pape, S.: Investigating Privacy Concerns related to Mobile Augmented Reality Applications – A Vignette Based Online Experiment. Computers in Human Behavior **122**, 106833 (sep 2021). https://doi.org/10.1016/j.chb.2021.106833, `https://linkinghub.elsevier.com/retrieve/pii/S0747563221001564`
27. Harborth, D., Pape, S., Rannenberg, K.: Explaining the Technology Use Behavior of Privacy-Enhancing Technologies: The Case of Tor and JonDonym. Proceedings on Privacy Enhancing Technologies (PoPETs) **2020**(2), 111–128 (2020). https://doi.org/10.2478/popets-2020-0020
28. Hassandoust, F., Akhlaghpour, S., Johnston, A.C.: Individuals' privacy concerns and adoption of contact tracing mobile applications in a pandemic: A situational privacy calculus perspective. Journal of the American Medical Informatics Association **28**(3), 463–471 (2021)
29. Henseler, J., Ringle, C.M., Sarstedt, M.: A new criterion for assessing discriminant validity in variance-based structural equation modeling. Journal of the Academy of Marketing Science **43**(1), 115–135 (2015). https://doi.org/10.1007/s11747-014-0403-8
30. Horstmann, K.T., Buecker, S., Krasko, J., Kritzler, S., Terwiel, S.: Who does or does not use the 'corona-warn-app'and why? European Journal of Public Health **31**(1), 49–51 (2021)
31. Horvath, L., Banducci, S., James, O.: Citizens' attitudes to contact tracing apps. Journal of Experimental Political Science pp. 1–13 (2020)
32. Huang, Y., Liu, W.: The impact of privacy concern on users' usage intention of mobile payment. In: International Conference on Innovation Management and Industrial Engineering. vol. 3, pp. 90–93 (2012)
33. Karahanna, E., Gefen, D., Straub, D.W.: Trust and TAM in Online Shopping: An Integrated Model. MIS Quarterly **27**(1), 51–90 (2003)
34. Kehr, F., Kowatsch, T., Wentzel, D., Fleisch, E.: Blissfully ignorant: the effects of general privacy concerns, general institutional trust, and affect in the privacy calculus. Information Systems Journal **25**, 607–635 (2015). https://doi.org/10.1111/isj.12062, `http://doi.wiley.com/10.1111/isj.12062`
35. Kostka, G., Habich-Sobiegalla, S.: In Times of Crisis: Public Perceptions Towards COVID-19 Contact Tracing Apps in China, Germany and the US. Tech. rep., Social Science Research Network, Rochester, NY (2020). https://doi.org/10.2139/ssrn.3693783
36. Krasnova, H., Spiekermann, S., Koroleva, K., Hildebrand, T.: Online social networks: Why we disclose. Journal of Information Technology **25**(2), 109–125 (2010). https://doi.org/10.1057/jit.2010.6, `http://dx.doi.org/10.1057/jit.2010.6`

37. Laufer, R.S., Wolfe, M.: Privacy as a Concept and a Social Issue: A Multidimensional Developmental Theory. Journal of Social Issues **33**(3), 22–42 (1977). https://doi.org/10.1111/j.1540-4560.1977.tb01880.x
38. Lee, H., Wong, S.F., Chang, Y.: Confirming the effect of demographic characteristics on information privacy concerns. In: PACIS 2016. p. 70 (2016)
39. Lewandowsky, S., Dennis, S., Perfors, A., Kashima, Y., White, J.P., Garrett, P., Little, D.R., Yesilada, M.: Public acceptance of privacy-encroaching policies to address the covid-19 pandemic in the united kingdom. PloS one **16**(1), e0245740 (2021)
40. Malhotra, N.K., Kim, S.S., Agarwal, J.: Internet users' information privacy concerns (IUIPC): The construct, the scale, and a causal model. Information Systems Research **15**(4), 336–355 (2004)
41. Meier, Y., Meinert, J., Krämer, N.: Investigating factors that affect the adoption of covid-19 contact-tracing apps. a privacy calculus perspective (2021)
42. Miranda, L.: How the coronavirus has widened the chasm between rich and poor. `https://www.nbcnews.com/business/business-news/how-coronavirus-has-widened-chasm-between-rich-poor-n1240622` (2020)
43. Munzert, S., Selb, P., Gohdes, A., Stoetzer, L.F., Lowe, W.: Tracking and promoting the usage of a covid-19 contact tracing app. Nature Human Behaviour **5**(2), 247–255 (2021)
44. Norberg, P.A., Horne, D.R., Horne, D.A.: The Privacy Paradox: Personal Information Disclosure Intentions versus Behaviors. Journal of Consumer Affairs **41**(1), 100–126 (jun 2007)
45. Oldeweme, A., Märtins, J., Westmattelmann, D., Schewe, G.: The role of transparency, trust, and social influence on uncertainty reduction in times of pandemics: Empirical study on the adoption of COVID-19 tracing apps. Journal of Medical Internet Research **23**(2), 1–17 (2021). https://doi.org/10.2196/25893
46. O'Callaghan, M.E., Buckley, J., Fitzgerald, B., Johnson, K., Laffey, J., McNicholas, B., Nuseibeh, B., O'Keeffe, D., O'Keeffe, I., Razzaq, A., et al.: A national survey of attitudes to covid-19 digital contact tracing in the republic of ireland. Irish Journal of Medical Science (2020)
47. Pape, S., Harborth, D., Kröger, J.L.: Privacy Concerns Go Hand in Hand with Lack of Knowledge: The Case of the German Corona-Warn-App. In: ICT Systems Security and Privacy Protection. SEC 2021. pp. 1–14 (2021)
48. Pavlou, P.A.: Consumer Acceptance of Electronic Commerce: Integrating Trust and Risk with the Technology Acceptance Model. Int. Journal of Electronic Commerce **7**(3), 101–134 (2003). https://doi.org/10.1080/10864415.2003.11044275
49. Podsakoff, P.M., MacKenzie, S.B., Lee, J.Y., Podsakoff, N.P.: Common method biases in behavioral research: a critical review of the literature and recommended remedies. Journal of Applied Psychology **88**(5), 879–903 (2003)
50. Ringle, C.M., Wende, S., Becker, J.M.: SmartPLS 3. `www.smartpls.com` (2015)
51. Schmitz, C.: LimeSurvey Project Team. `http://www.limesurvey.org` (2015)
52. Smith, H.J., Dinev, T., Xu, H.: Theory and Review Information Privacy Research: An Interdisciplinary Review. MIS Quarterly **35**(4), 989–1015 (2011)
53. Smith, H.J., Milberg, S.J., Burke, S.J.: Information privacy: measuring individuals concerns about organizational practices. MIS Quaterly **20**(2), 167–196 (1996)
54. Statista: Marktanteile der führenden mobilen Betriebssysteme an der Internetnutzung mit Mobiltelefonen in Deutschland von Januar 2009 bis September 2020. `https://de.statista.com/statistik/daten/studie/184332/umfrage/marktanteil-der-mobilen-betriebssysteme-in-deutschland-seit-2009/`

55. Voss, O.: Corona-App: Datenschutz-Debatte und offene Fragen. `https://background.tagesspiegel.de/digitalisierung/corona-app-datenschutz-debatte-und-offene-fragen` (2020)
56. Wagner, A., Olt, C.M., Abramova, O.: Calculating versus herding in adoption and continuance use of a privacy-invasive information system: The case of covid-19 tracing apps (2021)
57. Yang, H.C.: Young chinese consumers' social media use, online privacy concerns, and behavioral intents of privacy protection. Int. Journal of China Marketing **4**(1), 82–101 (2013)

All websites were last accessed on December 16th, 2021.

A Questionnaire

Demographics

AGE in years

EDU Education (no degree, secondary school, secondary school (>5 GCSE), A levels, bachelor, master, doctorate)

GDR Gender (female, male, divers, prefer not to say)

INCOME of household (in €: 0.5k-1k, 1k-2k, 2k-3k, 3k-4k, >4k, prefer not to say)

Smartphone Experience in years

Mobile OS Experience in years

USE Corona-Warn-App user (yes/no)

Privacy concerns related to the Corona-Warn-App[1]

PC1 I think the Corona-Warn-App over-collects my personal information.

PC2 I worry that the Corona-Warn-App leaks my personal information to third-parties.

PC3 I am concerned that the Corona-Warn-App violates my privacy.

PC4 I am concerned that the Corona-Warn-App misuses my personal information.

PC5 I think that the Corona-Warn-App collects my location data.

Perceived benefits of the Corona-Warn-App[1]

PB1 Using the Corona-Warn-App makes me feel safer.

PB2 I have a lot to gain by using the Corona-Warn-App.

PB3 The Corona-Warn-App can help me to identify contacts to infected individuals.

PB4 If I use the Corona-Warn-App I am able to warn others in case I am infected with Covid-19.

PB5 The spreading of Covid-19 in Germany can be decelerated by using the Corona-Warn-App.

Trust in the German healthcare system[1]

TRUST1 The German healthcare system is trustworthy.

TRUST2 The players acting in the German healthcare system are trustworthy.

TRUST3 The German healthcare system can cope with the burden of Covid 19 infections.

---

[1] measured on a 7-point Likert scale ("strongly disagree" to "strongly agree")