Less About Privacy: Revisiting a Survey about the German COVID-19 Contact Tracing App

Maximilian Häring
mhaering@cs.uni-bonn.de
University of Bonn
Bonn, Germany

Eva Gerlitz
gerlitz@cs.uni-bonn.de
Fraunhofer FKIE
Bonn, Germany

Matthew Smith
smith@cs.uni-bonn.de
University of Bonn, Fraunhofer FKIE
Bonn, Germany

Christian Tiefenau
tiefenau@uni-bonn.de
University of Bonn
Bonn, Germany

ABSTRACT

The release of COVID-19 contact tracing apps was accompanied by a heated public debate with much focus on privacy concerns, e.g., possible government surveillance. Many papers studied people's intended behavior to research potential features and uptake of the apps. Studies in Germany conducted before the app's release, such as that by Häring et al., showed that privacy was an important factor in the intention to install the app. We conducted a follow-up study two months post-release to investigate the intention-behavior-gap, see how attitudes changed after the release, and capture reported behavior. Analyzing a quota sample (n=837) for Germany, we found that fewer participants mentioned privacy concerns post-release, whereas utility now plays a greater role. We provide further evidence that the results of intention-based studies should be handled with care when used for prediction purposes.

CCS CONCEPTS

• **Security and privacy** → **Human and societal aspects of security and privacy**; • **Human-centered computing** → **Empirical studies in HCI**.

KEYWORDS

contact tracing, privacy, survey, intention-behavior-gap

ACM Reference Format:
Maximilian Häring, Eva Gerlitz, Matthew Smith, and Christian Tiefenau. 2023. Less About Privacy: Revisiting a Survey about the German COVID-19 Contact Tracing App. In *Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems (CHI '23), April 23–28, 2023, Hamburg, Germany.* ACM, New York, NY, USA, 16 pages. https://doi.org/10.1145/3544548.3581537

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. Copyrights for components of this work owned by others than the author(s) must be honored. Abstracting with credit is permitted. To copy otherwise, or republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee. Request permissions from permissions@acm.org.
CHI '23, April 23–28, 2023, Hamburg, Germany
© 2023 Copyright held by the owner/author(s). Publication rights licensed to ACM.
ACM ISBN 978-1-4503-9421-5/23/04…$15.00
https://doi.org/10.1145/3544548.3581537

1 INTRODUCTION

In 2020, the COVID-19 pandemic emerged fully. Many governments rolled out contact tracing apps in an attempt to fight the spread. Implementing contact tracing posed many challenges because it was never before carried out on such a scale. The hope was that a large portion of the population would install the apps since they are most effective if numerous people use them. So there was a great deal of interest in figuring out how many people would install such an app, what deters them, and how to motivate more people to do so. Many studies measured the acceptability and explored possible enablers or blockers for contact tracing apps [3, 32, 35, 65, 67]. Several of these studies focused on contact tracing in general and posed questions about hypothetical apps and features.

Unlike these studies which used fictitious apps and generic features, Häring et al. [32] specifically asked questions about an announced app, the Corona-Warn-App (CWA), released in Germany in June 2020, shortly after their study.

The authors found that even though the German government followed the more privacy-preserving decentralized approach after public discussions [55], 27.4% of the participants considered the app to be a threat to their privacy. Besides this, they found participants had many misconceptions about the app. The authors report that 50% of their participants reported they had some intention of installing the app. The study had been conducted before the app's release, so the authors could only gather statements about intended future behavior and beliefs about an app that was not yet available.

As intended and actual behavior show a gap in several research areas [49], we were interested in understanding how opinions and knowledge change after the release. We wanted to know whether participants used similar reasoning to justify why they had installed the app or refrained from doing so, compared to the intended behavior reported pre-release. With this, we shed light on the development of sentiments towards an app where the focus during development was on privacy and transparency.

We repeated the study done by Häring et al. [32] with minor adaptations in August 2020, two months after the release of the app in June. Like Häring et al., we conducted our study with a quota sample of the German population ($n = 837$).

We found that knowledge about the app had increased and beliefs about its surveillance capabilities had declined. While privacy concerns were not eliminated, they were no longer one main reason given by the participants to not install the app. Instead, the participants more commonly mentioned that they did not need the app or reported technical issues.

This work contributes to the body of knowledge in the following ways:

- We gather insights into reported show-stoppers that hindered the adoption of the app post-release.
- We compare these to the stated show-stoppers reported in the pre-release study by Häring et al. to evaluate how useful such hypothetical studies are in informing design and development decisions.
- We explore how knowledge, perceptions, and misconception improved post-release and discuss this in the context of the government's information campaigns, malfunctions, and general reporting.

The rest of the paper is structured as follows: In Section 2, we place our work in the context of related works. Further, we provide a short overview of the history and malfunctions of the German contact tracing app (CWA). In Section 3, we describe our methodology, especially compared to the original study by Häring et al. [32]. Section 4 presents the results of the replication in comparison to the original one. Finally, in Section 5, we discuss our findings and provide directions for future work.

2 CONTEXT AND RELATED WORKS

In this section, we first offer insights into the background of the German CWA, and changes made to the app between the original study and our repetition. We then provide an overview of studies on the knowledge and misconceptions about contact tracing apps. We also give an overview of the intention-behavior gap and reference studies examining the intentions to install a contact tracing app.

2.1 Background: Corona-Warn-App

Prior to the app's release in Germany, privacy had been a prominent topic in public discussions, amplified by the government's initial plan to build an app based on a central approach that was then discarded [58]. The CWA was finally introduced in June 2020 and follows a decentral approach for contact tracing based on the Exposure Notification System of Android and iOS [8, 15]. It uses Bluetooth to collect encounters with other devices [16] and no GPS data is gathered or used.[1] The development and operation costs for 2020 amounted to € 52.8 million [10]. The government promoted the app through an advertisement and education campaign [9, 31]. The app received positive feedback for its architecture [69] and criticism concerning the project's political handling [71].

After its release, the app continued to be a relevant topic in the media. There were frequent news reports about its functionalities or malfunctions in high-profile public (e.g., [57, 59, 70, 71]) and private media (e.g., [7, 51]).

Arzt et al. [6] captured the sentiment and discussion before and after the app's release by analyzing comments and reviews using natural language processing. They identified two peaks in the commenting activity: first, during the discussion about the app's protocol, and the other around the app's release. They clustered the arguments and found that the clusters "Politics" and "Privacy" occurred the most.

2.1.1 *Malfunctions of the App (known at the time of the study).*

As expected, the app was not free of technical problems. Between its release and our survey, the app was extended with additional features, languages, and fixes up to version 1.2.0 (released on August 7 2020) [30]. However, none of the core features changed.

In mid-July (around a month after the app's release), public broadcasters reported a problem with the app's capability to update the risk status when running in the background, both for Android [70] and iOS [57]. The app needed to be actively opened by the user to update the risk status. For Android, this problem arose because of the power-saving mode, especially problematic for smartphones produced by specific manufacturers. Since Version 1.1.1, released on July 20, 2020, users could access the device's settings over the app directly to allow their smartphone to run the CWA in the background [70]. For iOS, the developer of the CWA held Apple responsible but released a workaround in version 1.1.2 on July 24, 2020, which solved the problem [29]. Shortly thereafter, it became public knowledge that this problem had already been discussed on GitHub five days after the initial release of the CWA on June 16, 2020 [56].

Besides these, several minor issues, such as unhelpful error messages, were brought up by public broadcasters [71] or discussed on GitHub [26–28].

2.2 Knowledge Before and After the Apps' release

One of our goals with this study was to look at how peoples' knowledge developed over time. In this subsection, we list relevant work that studied knowledge about contact tracing apps.

Zetterholm et al. [67] provided a survey of studies concerning contact tracing applications. In particular, they referenced three studies that observed knowledge and misconceptions about such apps [50, 61, 68].

In these studies, participants, e.g., expressed uncertainty about an app about to be released in the UK [68] or showed technical (e.g., concerning the security of Bluetooth) or legal misunderstandings (US and Europe [50]). Different studies indicated that participants expected or believed the apps to have some kind of mapping that would allow users to see hot spots in the area or detect infected users nearby [32, 61, 68]. However, a majority of the participants had basic knowledge about contact tracing apps, and knew that the app would make it easier to contact people who had been exposed to Covid-19 [61] or that the Chinese solution would collect personal information and was controlled by the government [41].

To the best of our knowledge, only a few studies were conducted on the German contact tracing app (CWA) before and after its release.

Kozyreva et al. [38] drew four samples for a survey in Germany (n=4357): twice before the app's release and twice after it. Their focus was on digital contact tracing technologies in general, and they covered some aspects of the app. Even after its release, the fact that it used Bluetooth was known by only a minority of non-users (26% in the fourth sample) whereas 65% of the users were aware of it. The results of Meier et al. [42] were in line with this. Through

[1] For more information please visit the official website [15]. The source code of the app is available on GitHub [30].

a survey study of (non-)users, they found that knowledge about the app's privacy features positively relates to app usage. Häring et al. [32] carried out their study prior to the app's release and reported that 43.5% of the 657 participants who had heard about the app knew it would use Bluetooth, and 29.8% knew it would share IDs with devices in the vicinity of the smartphone. Only 9.9% knew all the information included in the official press release.

A study by Munzert et al. [43] tested in an experiment how interventions change participants' knowledge, their attitude towards the app, and app uptake. After being educated about the app, between 50 and 60% of the respondents knew that the app would not store the data it collected on a central server. In contrast, only around a third of the participants in the control group were aware of that. Interestingly, information had no big effect on the uptake but monetary incentives did.

2.3 Intention-Behavior Gap

An essential aspect of our study is comparing the reported intention in the pre-release study to the reported behavior in the post-release study, as well as the reasons given by the participants for their decision.

In general, the intention to do something is one of the strongest predictors of human behavior [1, 49]; yet not all those who want to do something actually do so. This difference between reported intention and actual behavior is known as the intention-behavior gap [2, 49]. While different studies and topics show different sizes of the gap, Sheeran et al. [49] reported that overall, about half of the people who intend to do something will act according to their plan. One reason for not acting as intended is that intention is not a one-dimensional construct. The basis upon which an intention is built can influence the likelihood of people acting on it. Examples are the extent to which an intention is relevant to the person's identity or whether an intention is built on personal beliefs, social pressure, or norms [49]. People also face challenges when they want to act on an intention, e.g., people often forget to act or miss opportunities [49].

In the HCI community, the gap between intention and behavior was already studied to build technology solutions for the various reasons that hinder people from acting on their intention (e.g., [4, 25, 46]), or understanding peoples' interaction with technical devices (e.g., [18]).

In the specific area of contact tracing apps, the reported intentions to use an app and the actual installation behavior also seem to diverge: During the development of contact tracing apps, researchers tried to predict whether developing the app would even be beneficial and what (socio-demographic) factors might influence app adoption. Online survey studies were conducted in which a hypothetical [65] or an upcoming app [32] was presented. These apps were then researched, e.g., by conducting discrete choice experiments and vignette studies. The Europe-wide acceptance of contact tracing apps (i.e., the willingness to install or just the general attitude towards the technology), as summarized by a meta-analysis of Zetterholm et al. [67], varied between studies and countries in the range of 38%-84%. Acceptance rates in Germany seem to lie in between: Kostka et al. [37] reported an acceptance rate of 41%, Häring et al. [32] reported 50%, and Altmann et al. [3] reported 60%.

However, Kozyreva et al. [38] identified that the installation rate of the CWA (36-41%) their participants reported was lower than the acceptability rate of the previously presented hypothetical scenarios (55-64%).

Jamieson et al. [36] researched this gap explicitly in the context of contact tracing and concluded that "over 50% of respondents who say they would probably or definitely install a contact tracing app would actually do so." They discussed that addressing privacy concerns is not enough to trigger installations, concurring with Munzert et al. [43] and Kozyreva et al. [38]. Jamieson et al. [36] discuss that social influences could play a relevant role in the installation behavior. For this, the authors distinguished between two kinds of social norms: injunctive (beliefs that one should install the app) and descriptive (believing that others installed the app).

Several of the challenges leading to the intention-behavior gap that Sheeran et al. [49] identified are intentions directed at habits. In the context of contact tracing apps, many of these challenges do not apply. One of the mentioned challenges is to set goals overoptimistically by, e.g., underestimating the amount of time needed to do something [49]. Yet, we assume that planning to install an app can be considered a simple and straightforward task for most users. Thus, this challenge should not come into play here. Additionally, people do not need to continue working on a habit change after they install an app, as contact tracing apps (for warning purposes) do not need to be actively used.

In this study, we provide insights into the intention-behavior gap in the case of a contact tracing app.

3 METHODOLOGY

Our methodology follows that of Häring et al. [32], with minor changes in the questionnaire, as explained below.

3.1 Survey Content

We used the survey by Häring et al. [32], conducted before the app was released; so we adjusted all tenses and answers accordingly. The survey consisted of the following seven parts. The complete survey text is included in the Supplementary Material.

3.1.1 Screening. As with Häring et al., our participants were required to use a smartphone and had to be older than 18. We sampled them according to age, income, education, and residence (federal state).

3.1.2 Media Sources and Knowledge. We asked the participants about their sources of information about the app (Q7[2]), what they believe is true for the app in general (Q8), and what applies to the app if they (Q10) or one of their contacts (Q9) is infected.

3.1.3 Usage. We provided the participants with a minimal description of the app, including a comprehension check question (Q11), and asked whether they had installed the app (Q12). In the original survey, the participants were asked how likely they were to use it. In our study, they could also indicate that they had uninstalled it or were planning to install it. We then asked for the primary reason (Q13).

[2] The notation Qx refers to the corresponding question in our questionnaire.

3.1.4 Previous Survey. It was not possible to recruit the same participants from Häring et al. again, but we used the same recruiting channel (Qualtrics); so there was a chance that we would get participants who had particpated in the pre-release survey. Therefore, we asked our participants whether they took part in the first study in May or June (Q14). If they answered "yes," we asked whether they had stated that they planned on using the app or not (Q15). If this did not match Q12, we asked for the reason for this discrepancy (Q16).

3.1.5 Change Motivators. Depending on their answer, we asked the participants what new functionalities or information about the app would change their view and would lead to an (un)installation (Q17). This question was not part of the original study.

3.1.6 Potential Properties. Häring et al. presented 24 statements of potential properties of the app and asked how these would affect the installation decision if they were implemented. Since this set of questions made no sense after release but we wanted to remain close to the original, we rephrased the questions to ask how these properties had affected their decision. Since not all properties were implemented and thus some were false, we gave participants the option of marking a statement as untrue. Since this made the questions fairly complex, we did not put much weight on its analysis.

3.1.7 Demographics. Finally, we asked for the participants' demographic data and how COVID-19 impacted their lives.

3.2 Recruitment

We followed the same recruitment process as Häring et al. [32]: Using Qualtrics [47], we aimed to draw a representative German sample according to age, education, household income, and residence (federal state). For this, we used the same quotas as Häring et al. The study was conducted from August 11 to August 27, 2020, two months after the app was launched on June 16, 2020. A total of 1001 participants completed the study for which we paid Qualtrics €4000.

3.3 Data Quality

As with the original study, Qualtrics excluded participants who 1) took less than half the median of the time participants needed in a final pilot study (244 seconds) for completing the survey or 2) gave an incorrect answer to the attention check question (Q18). We additionally excluded participants from our analysis who did not correctly answer the comprehension question (Q11). This step eliminated 164 participants. In total, the final data set consisted of 837 participants. The participants were asked what their highest vocational qualification was. All who answered with "Other" were manually sorted into one of the ISCED (International Standard Classification of Education) levels [64] based on the free text answers. If this was not possible, the qualification was set to "undefined."

3.4 Analysis

We had access to the data collected by Häring et al. [32] and followed their analytical approach to describe the participants' knowledge and their reported intention to use the app, respectively, in our case, their reported behavior.

In the following sections, to easily distinguish between the two data sets, we use `cwa_int` for the data collected by Häring et al. [32] and `cwa_beh` for the data gathered in our study.

In the sections where we evaluate participants' answers regarding their knowledge of the app, we excluded participants who had not heard about the app before (n = 11). We grouped participants by their current installation status. If they reported having uninstalled the app (n = 27), they were grouped as having the app not installed. Other answers ("Don't know" and "I don't want to state") were categorized as Unclear (n = 6).

3.4.1 Statistical Analysis. We replicated the exploratory analysis by performing a logistic regression with a model selection process using Akaike Information Criterion (AIC) and Bayesian Information Criterion (BIC.)[3] The initial set of factors consisted of all demographic factors, media sources, and the answers to each knowledge attribute. Before starting our study, we discussed possible hypotheses based on `cwa_int`. However, we did not think we had any good theoretical basis for expecting a restricted set of aspects to be different while expecting others to stay the same. This led to a huge amount of potential tests we could have hypothesized (with at least 26 attributes, an unforeseeable number of codes, and many demographic characteristics). As testing everything for differences did not seem a sensible option, we omitted further inferential statistics.

3.4.2 Qualitative Analysis. The survey included three open-ended questions (Q13, Q16, Q17). Those were coded. Answers to Q13 and Q17 were listed together in one document and provided additional context. Still, they were coded independently. As the survey was conducted in German, free text answers were translated for this paper.

Q13: Coding Reasons. We recoded the answers from `cwa_int` using the code book by Utz et al. [65] to make the data more comparable. To test whether the codes map well onto the given answers, four researchers coded the same 250 answers. In this step, we noticed that the question framing by Utz et al. [65] captured too much detail for our purpose. Further, the answers given by the participants (`cwa_int` and `cwa_beh`) were too vague and could thus fit into several sub-codes (e.g., making the distinction between "infection detection" and "infection prevention" was not always possible). Hence, we decided to reduce some of the codes. Additionally, due to the nature of the different questions the participants were asked, the meaning of some codes created by Utz et al. [65] needed to be expanded. The final code book is shown in Table 2 and provides examples of each code.

After deciding on the code book, we determined the inter-coder reliability of four researchers after they coded 110 answers (10.7% of the data, which is within the range recommended by Elder et al. to determine coder agreement [19]; the documents were selected randomly, as suggested by O'Connor and Jeffe [45]). We used ReCal3 [22] to calculate Krippendorff's alpha for each code. The inter-coder reliability for codes used at least twice was in the range of 0.13-1 with a weighted mean of 0.83 for `cwa_int` . The same procedure was repeated for the answers in `cwa_beh`. Again, we included all participants who completed the survey. For this,

[3]BIC is more restrictive than AIC. We used the model calculated by AIC because it contained all factors also present in the BIC model.

Krippendorff's alpha was in the range of 0.33-1 with a weighted mean of 0.96.

Finally, each researcher coded a fourth of all answers. Since some codes were covered only once or not at all in the data used for calculating the coder agreement, we subsequently discussed all documents coded with one of these codes or whose Krippendorff's alpha was less than 0.8.

We would like to note that some participants reported the German word "Sicherheit" as a reason, which can mean both "Safety" or "Security". If it was unclear what the participants referred to, the answers were assigned to the code "Unhelpful".

Q17: Coding Convincing Arguments. We asked what new functionalities or information would change the participants' decisions (convincing them to install or uninstall the app (Q17)). Four researchers coded 100 open responses, discussed their codes, and agreed on a final coding book. Two of them coded an additional 100 (10% of all) responses to calculate the inter-coder reliability using ReCal2 [21]. The remaining responses were split between the same two researchers. The final code book, including examples, can be found in the Supplementary Material. The inter-coder reliability (Krippendorff's alpha) for individual codes was 1 for all codes except surveillance (0.91) occurring in the subset. All codes, including examples and the code-specific inter-coder reliability, can be found in Table 1 in the Supplementary Material.

Q16: Coding Changed Opinions. We asked the participants whether they took part in the previous survey and, if they did, what intention toward app installation they had back then. If their answers did not match their current CWA installation status, they were asked why (Q16). As this scenario was relevant only to five participants, one researcher coded the answers and discussed the results with the rest of the authors.

3.5 Ethics

Our study was reviewed and approved by our institution's Research Ethics Board, and adhered to the German data protection laws and the GDPR in the EU. We provided an option for participants who did not want to give any details ("I don't want to state" or "I don't know") for all questions. Before taking part, the participants had to consent to their data being used for research. They could drop out at any time without any consequences. We excluded incomplete answers for the analysis.

3.6 Limitations

As in the case of every online survey study, this study has to work with some limitations. First of all, the data are self-reported. We cannot know for sure that the participants who reported having the app installed actually have it. Secondly, the study is potentially influenced by a recruitment bias. When the participants were invited to take part in the study, they already knew it would concern the CWA. Other studies found evidence that people who do not have the app installed are underrepresented in such studies [43]. Third, we set the same quotas as Häring et al. [32], but just like in their study, the recruitment by Qualtrics did not match it perfectly. Even though our sample is more representative than the previous study, it still did not achieve full representation for some demographic subgroups, such as participants older than 65 (cf. Table 1). This is a problem common to online surveys. When comparing `cwa_int` and `cwa_beh`, we not only looked at the overall numbers but also split them into subgroups to check that we do not misrepresent them. Lastly, it was not possible to recruit the same participants who took part in the study by Häring et al. Therefore, a direct comparison of intention vs. behavior per participant was not possible. To compensate for this, we worked with a large quota sample.

4 RESULTS

This section reports the results in the following way: a) Development of knowledge and misconceptions over time, and b) Comparison of the reported intention and reported action to install the app, including self-reported reasons mentioned for or against app installation.

4.1 Demographics

The participants were recruited as described in Section 3.2. We conducted recruitment considering quotas of age, education, income, and place of residence. A general overview of the demographics and their difference with those from `cwa_int` can be seen in Table 1.

The achieved quotas of the demographics differ between `cwa_beh` to `cwa_int`. Most notably, we had 9.4 percentage points more participants aged 65 or above, and 13.8 percentage points fewer participants in the age group of 18–24 years. Potentially related to this, we also see a difference between the data sets in income, work status, and self-assignment to the COVID-19 risk group. Related literature suggests differences between different demographic subgroups concerning app installation [67]. Thus, when presenting the results, we reported the overall numbers but checked whether the general trend is evident in all sociodemographic subgroups. We emphasize that even if a trend can be seen in all groups, the magnitudes vary. Therefore, we refer the interested reader to Tables 3 and 4, which show the detailed numbers of the participants based on their socio-demographics. Additionally, a visual representation of differences between `cwa_int` and `cwa_beh` for each group can be found in the Supplementary Material in Figure 1.

4.2 Knowledge And Beliefs

The participants were presented with 26 statements about the app, henceforth called "attributes," and were asked to mark all that apply to the app. Six attributes were true for the CWA at the time of the study, 15 did not apply to it, and five were neither true nor false but rather concerned a feeling or an intention. If we refer to one specific attribute, we use an identifier and mark them as such in the text for easier readability, e.g., `MANDATORY USAGE`. The complete statement represented by each identifier, its correctness, and the information whether it was mentioned in the official press release, can be found in the survey (Q8-10).

In the following paragraphs, we compare the number of participants from `cwa_int` and `cwa_beh` who marked correct statements about the app as true and the number of participants who expressed false beliefs about the app. An overview of the increase and decrease of percentage points in comparison to `cwa_int` is shown in Figure 1.

		int		beh		int		beh		int		beh
Gender (Q20)	**Female**	55.9	vs.	54.1	**Male**	43.3	vs.	45.6	**Other**	0.8	vs.	0.3
Age (Q1)	**18-24**	24.2	vs.	10.4 (9.2)	**25-34**	14.2	vs.	16.7 (15.3)	**35-49**	23.9	vs.	25.3 (23.9)
	50-64	26.7	vs.	27.2 (26.4)	**65+**	10.9	vs.	20.3 (25.1)				
Education (Q6)	**ISCED 0-2**	5.9	vs.	6.2 (16.5)	**ISCED 3-4**	48.9	vs.	56.8 (58.1)	**ISCED 5-8**	40.5	vs.	32.9 (25.4)
	Undefined	2.2	vs.	0.8								
Household Income (Q4)	**<= 1300€**	18.3	vs.	16.7 (16)	**1300-1700€**	13.4	vs.	7.5 (8)	**1700-2600€**	20.8	vs.	22.3 (20)
	2600-3600€	16.7	vs.	20.3 (18)	**3600-5000€**	14.0	vs.	20.4 (17)	**>5000€**	6.2	vs.	8.8 (20)
	Not disclosed	10.6	vs.	3.8								
Work Status (Q21)	**School student**	4.7	vs.	1.9	**Univ./col. student**	9.8	vs.	5.5	**Employee**	48.9	vs.	50.3
	Civil servant	2.0	vs.	3.0	**Self-employed**	4.6	vs.	4.1	**Freelancer**	2.2	vs.	1.1
	Unemployed	7.5	vs.	7.2	**Retiree**	16.9	vs.	25.0	**Not disclosed**	3.4	vs.	2.0
IT-Knowledge (Q22)	**Yes**	16.5	vs.	20.9	**No**	82.1	vs.	74.9	**Not disclosed**	1.4	vs.	4.2
Smartphone OS (Q3)	**Android**	72.0	vs.	71.5	**iOS**	26.0	vs.	26.1	**Other**	1.9	vs.	2.4
Political Affiliation (Q24)	**The Greens**	19.1	vs.	21.6	**CDU/CSU**	26.3	vs.	19.4	**SPD**	13.3	vs.	11.7
	FDP	5.1	vs.	6.0	**AfD**	7.3	vs.	6.7	**The Left**	11.2	vs.	10.1
	Others	17.7	vs.	24.5								
Federal state (Q2)	**BW**	12.3	vs.	12.9 (13.1)	**BY**	14.2	vs.	12.1 (15.6)	**BE**	4.9	vs.	7.0 (4.3)
	BB	3.1	vs.	2.4 (3.1)	**HB**	0.8	vs.	1.5 (0.8)	**HH**	2.7	vs.	3.6 (2.2)
	HE	7.6	vs.	6.9 (7.5)	**MV**	2.0	vs.	2.4 (2.0)	**NI**	9.8	vs.	6.7 (9.6)
	NW	23.1	vs.	22.8 (21.6)	**RP**	5.4	vs.	4.6 (4.9)	**SL**	1.2	vs.	1.5 (1.2)
	SN	4.4	vs.	5.0 (5.0)	**ST**	2.9	vs.	4.7 (2.8)	**SH**	3.1	vs.	3.5 (3.5)
	TH	2.4	vs.	2.4 (2.7)								

Table 1: Participants' demographics ($n = 837$), in percentages. Gray: Percentages from `cwa_int` ($n = 744$). Numbers in brackets represent the targeted distribution [17, 47].

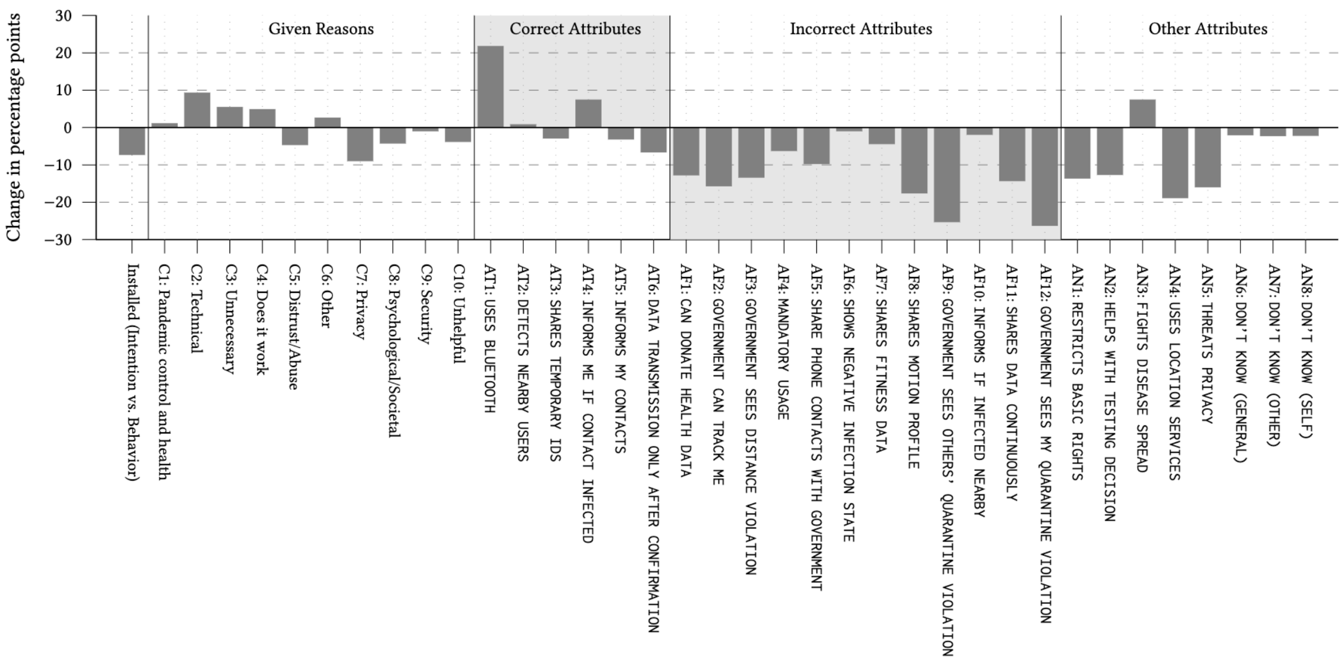

Figure 1: Gains and losses in p.p. of high-level codes, attributes, and app installation intention and action. If a bar is in the area with a gray background, more participants in `cwa_beh` than in `cwa_int` had correct knowledge about this specific attribute. We can see this is the case for most attributes. "Reasons" and "Other Attributes" do not concern knowledge; therefore, we cannot make such an assessment. In Q8-10, participants could answer that none of the given attributes were correct. Only a very small amount (up to 2.6%) marked that, so they were excluded from the Figure.

4.2.1 Knowledge about the app increased. Despite the divisive nature of the many COVID-19 measures [54] and the disinformation targeted at them [66, 72], it is nice to see that knowledge about the app increased while misconceptions declined. Häring et al. [32] measured how many participants correctly checked every point mentioned in the official press release regarding the app. They reported that 9.89% of the participants did so. As FIGHTS DISEASE SPREAD is something that can be argued about, we decided to recalculate the number without this. Following this, 10.8% of the participants who heard about the app knew the basics in `cwa_int`, and 13.6% in `cwa_beh`.

In detail, the degree to which knowledge about the app increased differs. **Contact tracing** as the essential purpose of the app was known to the majority of participants: INFORMS MY CONTACTS, which was already known by a majority in cwa_int, was known by even more participants in all demographic subgroups, with an average of 78%. However, the other direction of contact tracing, INFORMS ME IF CONTACT INFECTED, did not rise in all subgroups, despite still being known by 70.5%. As described in Section 2.1.1, not actively opening the app might have led to the participants not being informed timely. This issue could have resulted in the participants believing that they would not be warned about contact with an infected person.

Two attributes stated **technical properties**. That the app uses Bluetooth (USES BLUETOOTH), which was included in announcements of the app (e.g., [8]) and which can be noticed when using the app, was marked by 65.4%. This is a rise from cwa_int where it was 43.7%. The number of participants aware of the rather specific technical fact that the app shares temporary IDs (SHARES TEMPORARY IDS) with other devices remained very similar between cwa_int to cwa_beh and was known by a minority (29.8% and 26.9%).

4.2.2 Fewer (privacy) concerns. The attributes included statements concerning the app giving the government access to phone contacts, the sharing of a motion profile, the government seeing users' current location, and the government noticing violations of social distancing protocols or quarantine rules. Reasonably, all of them could be seen as an intrusion of privacy. Compared with cwa_int, we see fewer participants believing these to be true. For example, the belief SHARES MOTION PROFILE, which was marked true by 41.8% of the participants of cwa_int, was now checked by 24.1% in cwa_beh.

In cwa_int, 27.3% expressed concerns about their privacy (THREATS PRIVACY) due to the app's installation/usage, 20% even saw their basic rights restricted (RESTRICTS BASIC RIGHTS). Both concerns declined significantly in cwa_beh (11.4% and 6.4% respectively).

4.2.3 Misconceptions. This section gives an overview of the misconceptions people expressed in form of free text answers.

Even though fewer participants marked the app as a threat to their privacy (THREATS PRIVACY), the concern was not dispelled entirely: In both data sets, we saw participants who were certain that the app has features or collects data that would invade their privacy.

For example, participants expressed the belief that it is possible to receive a real-time warning about infected people in the users' surroundings. This misconception was also included in the attributes (INFORMS IF INFECTED NEARBY): 55.7% of the participants believed this. If true, this would be an actual threat to users' privacy. However, only 10.9%, who marked this attribute to be accurate, indicated the app to be a threat (THREATS PRIVACY). To the best of our knowledge, neither the app design nor any of the official information about the app would imply such functionality.

It was also brought up that users would be informed who among their contacts is infected. Broadly, participants felt that the app would violate a law or that it would be used to track or spy on its users. Emphasizing an incorrect understanding of what data the CWA can access, people mentioned the sharing of personal data in response to the question asking for reasons that could change their current opinion (Q17). Some participants gave the impression that they believed the app already has access to these data: "when my phone number is disclosed" or "If it were to share my personal information or my location."

The participants thought it would be necessary to have mobile data to be able to use the app. While the app needs an internet connection to download keys from users who shared their positive infection status, this does not need to be performed constantly. Further, German network operators agreed not to charge for the CWA data usage [44].

The participants from both data sets mentioned that Bluetooth is insecure. While we could not identify the origins of the notion, it could be that participants had heard about vulnerabilities associated with Bluetooth, e.g., BlueBorne [5], and transferred those. Since we do not know what device the participant owned, this is not necessarily a misconception.

Misconceptions only present in the cwa_int. Only in cwa_int did we see participants who based their decision on whether to install on beliefs that were grounded on the fact that the app had not yet been released and some political decisions were still being discussed. The participants, e.g., thought that quarantine would be enforced after receiving a warning or that it would be mandatory to use the app. While the latter belief was also observed in the attributes in cwa_beh, no participant used it as an argument for why they had not installed the app. On the other hand, participants mentioned that they had installed the app due to social pressure (e.g., from their spouses or employer).

The participants also communicated beliefs leading to a false sense of safety, e.g., that the app prevents users from infecting others or that it provides safety against infection.

New Misconceptions. A new theme in cwa_beh was that only a perfect app or its perfect usage would lead to success: "For this, I must ALWAYS have my phone with me, and that is too laborious for me." Additionally, we now saw participants who either believed it was "proven" that the app did not work or produce the effect aimed for. One participant came to this conclusion based on personal experience after not receiving warnings: "I was [...] downtown, and the app didn't show any warnings at all [...]. It is very unlikely that I was not in contact or in the vicinity of anyone who had Corona."

4.3 Reported Intention vs. Action

We repeated the survey when the CWA had already been released, so we had to adjust some questions and therefore measure different concepts. While in cwa_int, the participants reported their installation intention, cwa_beh asked for their installation behavior. In this section, we compare the reported intention, reported behavior, and download numbers.

Figure 2 provides an overview of the overall installation intention (cwa_int) and action (cwa_beh). Around 45.9 % of the participants reported having had the app installed at some point in time ("Yes" (42.7%) or "Yes, but uninstalled" (3.2%)). Comparing this to the download numbers, it seems that people who have installede the app were more likely to participate in the study. At the end of this study, the CWA had 17.6 million reported downloads (August 27, 2020 [14])[4], which translates to 28.98% of the smartphone users

[4]Download numbers are only an estimation of the installation numbers. E.g., uninstallations and reinstallations are not recorded.

in Germany (60.74 Mio., based on an estimation from 2020 [53]). This is less than both the measured intention in cwa_int and the reported installations in cwa_beh.

In cwa_int, 18.2 % were undecided on whether or not to install the app. As the app was not installed automatically, the default option is not to install it. On an aggregated level, it seems that more people who were undecided "chose" not to install the app.

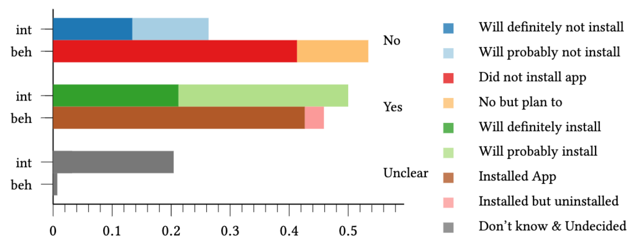

Figure 2: Installation intention (int) as reported in cwa_int vs. installation behavior (beh) as reported in cwa_beh.

4.3.1 *Influence of Knowledge on App Installation.* Häring et al. [32] reported statistically significant exogenous variables of a regression that influenced the participants' intention to install the CWA. We repeated the analysis and performed a logistic regression. The full resulting model and the model of cwa_int are reported in the Supplementary Material in Table 1.

In the following paragraphs, we focus on the knowledge and belief factors measured with the attribute questions (Q8-10) to determine whether they influence the participants' decision to install the CWA. Some of the selected attributes overlap for both data sets.

The **knowledge** that the app will inform the user's contacts if they tested positive (INFORMS MY CONTACTS, Log Odds = 0.86), that some authority has to confirm a positive test result before it can be shared over the CWA (DATA TRANSMISSION ONLY AFTER CONFIRMATION, Log Odds = 0.52), and that the app uses Bluetooth (USES BLUETOOTH, Log Odds = 1.13) positively influence app installation. The first two factors were also found in cwa_int.

Two attributes that **do not apply to the app** statistically significantly increased app adoption as well: Believing its usage was mandatory (MANDATORY USAGE, Log Odds = 3.73) and thinking the app could be used to prove a non-infection status (SHOWS NEGATIVE INFECTION STATE, Log Odds = 0.49).

We also identified **beliefs** that hindered adoption: Participants who believed the app to be a threat to their privacy (THREATS PRIVACY, Log Odds = −4.50, also included in the model for cwa_int) or thought the app would enable the government to gather information on the apps' users (SHARE PHONE CONTACTS WITH GOVERNMENT, Log Odds = −2.97, GOVERNMENT SEES MY QUARANTINE VIOLATION, Log Odds = −1.20, GOVERNMENT SEES DISTANCE VIOLATION, Log Odds = −0.98) were statistically less likely to install the app. THREATS PRIVACY had the largest effect size. Around 97% of the participants who believed this did not install the app, whereas 99.5% of those who installed the app at some point did not state to feel a threat to their privacy.

4.3.2 *Reasons Given.* In the following paragraphs, we present the most common motivations participants mentioned for or against the installation of the CWA, as shown in Table 2.[5] A visualization of the increase and decrease is included in Figure 1. The C* notation in this section refers to the Figure.

Pandemic Control as Primary Motivator. As could be expected, most people who had the app installed did so to contribute to the pandemic control (C1) in some way or the other (73.7%). These ranged from social reasons (protecting others) to more self-focused ones, such as protecting oneself. This number is not far away from those seen in cwa_int: 73% of those who were very certain about installing the app reported the pandemic as a reason (61% of those who intended to likely install).

Fewer Distrust and Privacy Concerns. In cwa_int, the two most commonly mentioned reasons why participants did not want to install the app were privacy (C7) and the fear of it being used for something else (C5). Both topics were also brought up by participants who were undecided about whether they wanted to use the app. In cwa_beh, the general notion of distrust (e.g., concerning the government, developers of the app, or the belief that the app will be used for something other than what was advertised, such as surveillance; C5) and privacy/security concerns (C7, C9) were mentioned by fewer participants. This declining trend is observed in almost all demographic groups, albeit in varying degrees. There is one outlier for distrust which is the income group 1300-1700€ (cf. Table 4 or Figure 1 in the Supplementary Material).

While fewer privacy concerns were mentioned overall, we still came across participants who, at the time of the study, believed that the app collects or even uses data it does not need. When asked what new features or information would convince them to install the app, seven participants self-reporteded that they would install the app if it stopped collecting data it does not need or stopped monitoring its users. It should be noted that while privacy concerns were less frequently mentioned, the participants who had installed the app still cared for their data: 35.6% stated they would uninstall the app if any changes to its data protection, security, or usage of the data were made. Only three participants explicitly mentioned changing the app's approach from the current one to a centralized one as the reason for them to uninstall.

Technical Issues Hinder Usage. The increase in the number of people from all socio-demographic subgroups who reported that **technical reasons** led to not having the app installed (overall from 2.8 to 12.2 %) was rather large. Specifically, the participants mentioned that their operating system (OS) does not support the app, or it is just too slow. Bluetooth was also brought up, either because the participants were unsure whether it is secure, resulting in them not wanting to enable it or because they feared the app would drain the battery too much. The increase in technical reasons was especially high for participants aged over 65 (cf. Figure 3, C2).

Notably, 52% of the participants who uninstalled the app reported technical reasons. For instance, they experienced battery problems due to Bluetooth or criticized the app for using up their phone's memory.

[5]To facilitate comparison with our results, we referenced other studies that reported the same theme in the Table.

Of the 39 participants, who had also answered the first survey, five reported they had intended to install the app but did not currently have it installed. Three participants mentioned that their phone does not support the app, and one had tried but failed to install the app. Although technical limitations would have been known before the release, e.g., the use of an OS that is not supported, we think it is not plausible to assume that many people thought about this at the time of that study.

Skepticism About Apps' Capabilities. The notion that the app is **unnecessary** (C3) increased especially due to participants personal assessment of their own behavior. Specifically, the participants mentioned that they never or rarely left their residences or that the time they spent close to strangers was too short to receive a warning anyway. Only a few participants questioned the severity or existence of COVID-19.

We also saw a slight increase in the percentage of participants who were unsure about or **doubted whether the app works** as promised (C4). For example, they mentioned technical malfunctions (only three mentioned a specific problem), stated that the user base is too small, or that they doubted that everyone would share their positive infection status over the app. When asked what functionality could lead to an installation, 7.2% mentioned they would install the app if it malfunctioned less. Again, most of these statements were vague, and only three participants pointed to specific problems, such as a QR-Code scanner that did not work or the app not working properly in the background, as mentioned in Section 2.1.1.

Few Reasons Were Given to Change Installation Status. As many as 46.0% of the participants who answered the question of how their current installation status could be changed (n=730), stated that no new information or functionality could convince them to change their opinion. Of these, 43.2% participants had installed the app, whereas 56.8% did not. Four participants mentioned that even the use of more data, probably resulting in the app being less privacy-preserving, would not tempt them to uninstall it.

Another 7.8% said they "don't know" what could change their minds; this means that they, at the time, found no factor that would influence their decision.

5 DISCUSSION

We revisited a survey study shortly after the release of the German CWA to measure the development in the knowledge and beliefs of participants, and whether the previously reported intentions to install the app resulted in actions. We found fewer participants who reported having the app installed in `cwa_beh` than those who reported intending to do so in `cwa_int`. Both numbers differed from the estimated actual installation numbers based on downloads. We found that the reasons shifted with varying degrees for different socio-demographic groups. In the following paragraphs, we discuss these findings.

5.1 Privacy and Ideological Reasoning

When Häring et al. [32] conducted the original survey, the apps' privacy was a big issue. In April 2020, organizations dealing with internet politics (including the "Chaos Computer Club"[13] and the "Gesellschaft für Informatik" [23]) wrote an open letter to the German Chancellery, strongly encouraging them to distance themselves from the centralized approach planned at first for a contact tracing app. They claimed that people would not trust such an app and, hence, not install it [12].

Arzt et al. [6], who analyzed comments from three German online newspapers, Twitter, and app stores before and after the release of the CWA found that the second most frequently brought-up topic concerned privacy. The literature in which German participants were asked about contact tracing apps also identifies a lack of privacy to be one of the leading negative associations [3, 38, 65]. In the previous study [32], 27.4% of the respondents thought the app would be a threat to their privacy, and the two main reasons that the participants from `cwa_int` used to justify not intending to install the app were "Privacy" and "Distrust/Abuse."

We Saw Fewer Privacy Concerns ... When we asked our participants about the main reason for not having the app installed, in general, fewer participants argued with privacy or trust. As summarized in Section 2.1, the apps' technical details did not change substantially between the two studies to explain the discrepancy in the number of privacy-related concerns. We thus believe that there are other possible explanations for this decline.

First, Munzert et al. [43] experimented with educating their participants. They could see that their intervention (videos explaining app functionality, claims about data privacy, and the benefits of the app for either the participant or vulnerable populations) had a statistically significant positive effect on both the participants' knowledge and their attitudes towards the app. Installation numbers also slightly increased, but not in all of the groups. Consequently, what we see in the data could be an effect of effective advertisements for the app (such as [9, 31]). These advertisements not only explained the apps' functionality and data handling but also tried to convince people that installing the app helps combat the pandemic [63]. So, alongside the extreme presence of the pandemic in the media and in daily life, the advertisement likely contributed to social influences such as an injunctive norm that people should install the app (cf. Jamieson et al. [36]).

Second, there might be a portion of the population who, for ideological reasons, did not want to install the app and used privacy as a convenient straw man to justify their position. Since a lot of effort was put into assuaging the privacy concerns, this portion of the population might have switched to another reason for not installing the app, such as not needing it.

...But They Are Still Relevant. Although the trend shows fewer privacy concerns (27.4% `cwa_int` vs. 11.4% in `cwa_beh`), they were not eliminated, and still connected to being less likely to install the app. We assume that for participants who felt so, privacy concerns were still an important reason not to install the app. And vice versa, most participants who installed the app did not think it threatened their privacy. As the technical details of the app, including its data handling, addressed many privacy issues by design, we need more insight into what privacy means to different groups and how concerns are built or broken down in this context.

Prior research has already used known instruments to measure the concept of privacy concerns and relate them to app usage: Utz et al. [65], e.g, used the IUIPC, Seeberger et al. [48] the MUIPC, and Jamieson et al. [36] used UTAUT. These studies teach us how general concerns relate to intention and behavior, but they do not tell us what the concerns are and where they originate from when looking at contact tracing apps specifically.

It seems that even beliefs that can be reasonably seen as privacy-invasive are not always considered as such: Kulyk et al. [39] found that 71.9% of their German participants believed the app used meta-data, such as the geo-location, whereas only half of this percentage marked to be concerned about privacy, being unclear whether all those who were concerned also believed the app to capture this data. Both `cwa_int` and `cwa_beh` show something similar: more participants believed the app would share a motion profile or thought it would inform them if infected people were nearby than who marked the app as a threat to their privacy.

We also assume that the phrasing of a question is likely to have a huge impact on the answers: while only 11% of the participants were unwilling to download the app if it was used for finding hotspots in the study by Kulyk et al. [39], 45% were not comfortable with sharing their location data with the authorities in case they were infected to enable them to publish such hotspots.

What seems appropriate or not is also highly context dependent [40], and thus, it is hard to assess what notion of privacy (e.g., informational, interactional, or social [40]) the participants' answers are based on. Here, we suggest researchers to distinguish between those in their work.

Based on vignette studies, such as that of Utz et al. [65], we know which features and data-sharing characteristics people (dis)like. However, as mentioned, many negatively connotated characteristics are not included in the actual CWA. So, to understand why 11.4% still believed the app to be a threat to their privacy, we suggest researchers ask more directly about details participants assume to be an issue and whether they believe these details are currently part of the app.

Many Marticipants Were Certain About Their Decision. What did remain constant between the original study and our replication was the absolute certainty of participants. Häring et al.'s [32] title summed it up: "Never ever or no matter what". The same is still valid; many of the participants in our sample (n = 336, 46%) were very sure about their decision of having or not having the app installed and said that nothing could change their minds.

5.2 Reasons To Install Or Not: Perfect Is The Enemy Of Good

The reported reasons for or against installing the CWA were a lot more specific in `cwa_beh` than in `cwa_int`. After the app was released, the participants evaluated their need for the app and its possible positive and negative effects. In the end, many of the participants decided against installing it. When asked, some brought up the lack of necessity, as they barely leave their homes or are not in contact with strangers long enough for an infection to occur. Participants also argued that they do not always carry their phones with them. Similarly, Altmann et al. [3] observed that the people who have their phones on them more often were more likely to support the app.

The hope was to have as many installations as possible. Sometimes it was misreported that 60% of the population would need to install the app for it to be effective [60], which created a measure against which success was judged. It can be certainly said that it is beneficial to have a high user base so that it is more likely that the person a user meets also has it installed. 60% was estimated to be the threshold for the app to stop the pandemic. Nevertheless, even low adoption rates can reduce the number of COVID-19 cases and deaths [33, 60]. How many people can have what effect depends significantly on the specifics of the virus variant and other non-pharmaceutical interventions.

If the goal is to increase overall adoption, it may be interesting to further research possible interventions. Böhm et al. [11] did so. They found that the official video lead to a significant increase in perceived usefulness but not in behavioral intention. Just explaining how the app works is not enough to increase adoption intention. The perception of usefulness may also vary depending on the situation of the user and the provided specific function (cf. Lu et al. [40]). In the beginning, the CWA only served the purpose of contact tracing (via Bluetooth). Over the years, it has offered a lot more, such as a manual contact diary function, a certificate wallet, and information about the local COVID-19 situation. We think it is noteworthy that the lack of utility of the app was brought up more often in `cwa_beh` than in `cwa_int`. This finding is in line with that of Böhm et al. [11].

5.3 Lost Once, Lost Forever?

Around 12% of the participants reported technical reasons for not installing the app. Not using a buggy or broken app seems to be a very logical view. However, we identified two problems. First, many published bugs were relevant only to a small population [26–28]. Second, it opens up the question of how it can be communicated that a particular bug is eliminated if the app has not been installed and the non-user is no longer paying attention.

Many participants did not mention a specific problem but "malfunctions" in general. We assume that at least some referred to the background synchronization problems, as they were discussed in the media shortly before the study. However, it had already been resolved by the time of the survey. We assume that some of the participants were not aware of the new release that solved the corresponding problem. In a typical software development cycle, a roll-out to early adopters or even open betas can gather feedback and be used to adapt to emerging problems. However, in 2020, the situation required immediate action. So, in the case of the CWA or any app developed in a short time, such early roll-out was not possible.

This problematic situation points to the question: Is our current technological landscape able to help in such situations (fast enough)? It may seem obvious that there should be as few bugs as possible in such an application. But still, with all the devices that must be supported, it is fair to assume that bugs do exist. At the same time, we are not aware of any research on how many uninstalled the app after encountering a bug and whether this is an uninstall reason or more of a reputation problem.

5.4 Lesson Learned from Replicating an Intention Study

5.4.1 Provide more context in studies about intention and handle results with care. Our analysis shows that the reported intention to install in cwa_int was only slightly higher than the reported installation numbers in cwa_beh (50% vs. 45.9%). When we compare our reported installation numbers (45.9%) with those of Kozyreva et al. [38] and Munzert et al. [43] (both around 40%, utilizing representative samples recruited at different times between August and November 2020), the numbers seem mostly consistent across these studies. While the studies were conducted, the download numbers did go up [52], but we cannot say for sure how exactly this relates to the installation numbers. Contrary to the numbers previously reported by Häring et al. [32], Kozyreva et al. [38], and Munzert et al. [43], Kulyk et al. [39] found that 72.7% of their German participants (smaller sample recruited between December 2020 and February 2021) stated to have installed the app at some point. In conclusion, we find that the installation numbers (reported behavior) in each of these samples are not the real user numbers (actual behavior). Based on the number of downloads, we assume the reported behavior is around twice as high as the actual behavior.

Jamieson et al. [36] compared the reported intentions and reported behavior of participants based in the USA. The authors estimated that around 50% of those with an intention to install would do so but without comparing it to corresponding download numbers of available apps.

Comparing the percentages of cwa_beh and cwa_int, our (reported) intention-behavior proportion would be 91.8% compared to the 50% reported by Jamieson et al. [36]. Yet, we cannot say where the offset originates from.

To make a comparison of the data easier and more meaningful, we ask researchers to put their (reported intention and behavior) numbers in the specific context (recruiting method, intention-behavior gap, observable actual behavior) as much as possible. This obviously cannot always be done directly: Reporting about installation behavior before the release is impossible. Following this, policy-makers should be cautious when using numbers as a ground for or against features without further knowledge about the context, e.g., the gap between reported and actual behavior.

Nonetheless, we think that conducting intention studies still offered an interesting and important view on the topic.

5.4.2 Age. Related work found a contradictory influence of participants' age. While Altmann et al. [3] found younger participants more willing to install a contact tracing app, the literature also offers the opposite finding [43, 67].

While age was not selected in the presented regression as a predictive factor, participants who were 65 or older had higher percentages for their installation intention in cwa_int compared to all other age groups (cf. Table 3). This group also had the highest loss in percentage points (22.9) when it comes to actual installation numbers. The code "Technical" (including both not being able to install the app as well as using one's phone in a way that clashed with app usage) was the most mentioned reason why the app was not installed in this group. Percentage-wise, it was also more frequently mentioned by this group than by other groups. This seems especially problematic for the following reasons: a) this age group is quite large, not only in Germany, b) the members of this group might be classified to be at a higher risk due to the virus; and c) older people are often talked about, but not always included in conversations [24]. While it might be challenging, we strongly encourage researchers to actively recruit older participants for such studies.

6 CONCLUSION

We replicated a study by Häring et al. [32] about the Corona-Warn-App and measured the knowledge, installation status, and reasoning in the German population with a quota sample (n=837). In contrast to the original study, we surveyed after the app's release. We compared both survey data sets. More participants reported that they intended to install the app than reported having installed the app. However, both these numbers are higher than estimated based on the official download numbers. Knowledge increased, and false beliefs declined, especially concerning the surveillance capabilities of the app. We encountered fewer privacy concerns and less distrust in the involved parties. Looking at the reported reasons for the installation decision, we found that many participants who did not install the app gave technical problems or a personal estimation of the usefulness or necessity of the app as the reason.

ACKNOWLEDGMENTS

We thank the Werner Siemens-Stiftung (WSS) for their generous support of this project. We thank Julia Angelika Grohs, Bilal Kizilkaya, and our anonymous reviewers for their help and feedback.

REFERENCES

[1] Icek Ajzen. 1991. The theory of planned behavior. *Organizational behavior and human decision processes* 50, 2 (1991), 179–211.
[2] Icek Ajzen. 2011. The theory of planned behaviour: Reactions and reflections. *Psychology & health* 26, 9 (2011), 1113–1127.
[3] Samuel Altmann, Luke Milsom, Hannah Zillessen, Raffaele Blasone, Frederic Gerdon, Ruben Bach, Frauke Kreuter, Daniele Nosenzo, Séverine Toussaert, and Johannes Abeler. 2020. Acceptability of App-Based Contact Tracing for COVID-19: Cross-Country Survey Study. *JMIR mHealth and uHealth* 8, 8 (2020), e19857. https://doi.org/10.2196/19857
[4] Leonardo Angelini, Elena Mugellini, Omar Abou Khaled, Christina Röcke, Sabrina Guye, Simone Porcelli, Alfonso Mastropietro, Giovanna Rizzo, Noemi Boqué, Josep M del Bas, Paula Subias, Silvia Orte, and Giuseppe Andreoni. 2019. The NESTORE E-Coach: Accompanying Older Adults through a Personalized Pathway to Wellbeing. In *Proceedings of the 12th ACM International Conference on PErvasive Technologies Related to Assistive Environments* (Rhodes, Greece) *(PETRA '19)*. Association for Computing Machinery, New York, NY, USA, 620–628. https://doi.org/10.1145/3316782.3322763
[5] Armis. 2021. *BlueBorne.* Armis. Retrieved February 17, 2022 from https://www.armis.com/research/blueborne/#/technical
[6] Steven Arzt, Andreas Poller, and Gisela Vallejo. 2021. *Tracing Contacts With Mobile Phones to Curb the Pandemic:Topics and Stances in People's Online Comments About the Official German Contact-Tracing App.* Association for Computing Machinery, New York, NY, USA, 1–7. https://doi.org/10.1145/3411763.3451631
[7] Bild. 2020. *Was bei Fehlermeldungen der Corona-App zu tun ist.* Axel-Springer-Verlag. Retrieved September 6,2022 from https://www.bild.de/digital/smartphone-und-tablet/handy-und-telefon/falsche-region-fehlermeldungen-der-corona-warn-app-so-reagieren-sie-71575830.bild.html
[8] Bundesregierung. 2020. *Veröffentlichung der Corona-Warn-App.* Bundesregierung. Retrieved February 17, 2022 from https://www.bundesregierung.de/breg-de/suche/veroeffentlichung-der-corona-warn-app-1760892
[9] Bundesregierung. 2020. *Wie funktioniert und was kann die Corona-Warn-App?* Bundesregierung. Retrieved February 17, 2022 from https://www.bundesregierung.de/breg-de/themen/corona-warn-app/corona-warn-app-erklaerfilm-1758828
[10] Presse Bundestag. 2022. *Mehr als 130 Millionen Euro Kosten für die Corona-Warn-App.* Bundesregierung. Retrieved February 17, 2022 from https://www.bundestag.de/presse/hib/kurzmeldungen-877736
[11] Victoria Böhm, Christian Wolff, Corinna Geiselhart, Eric Karl, and Nina Kleindienst. 2021. Investigating Barriers for the Adoption of the German Contact-Tracing App and the Influence of a Video Intervention on User Acceptance. In

Mensch Und Computer 2021 (2021-09-05). ACM, Ingolstadt Germany, 330–337. https://doi.org/10.1145/3473856.3474017
[12] Chaos Computer Club. 2020. *Corona-Tracing-App: Offener Brief an Bundeskanzleramt und Gesundheitsminister*. CCC. Retrieved February 17, 2022 from https://www.ccc.de/de/updates/2020/corona-tracing-app-offener-brief-an-bundeskanzleramt-und-gesundheitsminister
[13] Chaos Computer Club. 2022. *CCC | Home*. CCC. Retrieved February 18, 2022 from https://www.ccc.de/en/
[14] Corona-Warn-App. 2020. *Kennzahlen zur Corona-Warn-App*. Robert-Koch-Institut. Retrieved February 17, 2022 from https://www.coronawarn.app/de/analysis/
[15] Corona-Warn-App. 2022. *Open-Source-Projekt Corona-Warn-App – FAQ*. Robert-Koch-Institut. Retrieved September 6, 2022 from https://www.coronawarn.app/en/faq/
[16] Corona-Warn-App. 2022. *So funktioniert die App am besten*. Robert-Koch-Institut. Retrieved September 6, 2022 from https://www.coronawarn.app/de/#howto
[17] Destatis. 2022. *Einnahmen und Ausgaben privater Haushalte*. Statistisches Bundesamt. Retrieved February 17, 2022 from https://www.destatis.de/DE/Themen/Gesellschaft-Umwelt/Einkommen-Konsum-Lebensbedingungen/Einkommen-Einnahmen-Ausgaben/_inhalt.html
[18] Serge Egelman, Marian Harbach, and Eyal Peer. 2016. Behavior Ever Follows Intention? A Validation of the Security Behavior Intentions Scale (SeBIS). In *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems* (San Jose, California, USA) *(CHI '16)*. Association for Computing Machinery, New York, NY, USA, 5257–5261. https://doi.org/10.1145/2858036.2858265
[19] Glen H Elder, Eliza K Pavalko, and Elizabeth Colerick Clipp. 1992. *Working with archival data: Studying lives*. Vol. 88. Sage Publications, Inc., Thousand Oaks, California.
[20] Grace Fox, Trevor Clohessy, Lisa van der Werff, Pierangelo Rosati, and Theo Lynn. 2021. Exploring the competing influences of privacy concerns and positive beliefs on citizen acceptance of contact tracing mobile applications. *Computers in Human Behavior* 121 (Aug. 2021), 106806. https://doi.org/10.1016/j.chb.2021.106806
[21] Deen Freelon. 2022. *ReCal2: Reliability for 2 Coders*. Deen Freelon. Retrieved February 17, 2022 from http://dfreelon.org/utils/recalfront/recal2/
[22] Deen Freelon. 2022. *ReCal3: Reliability for 3+ Coders*. Deen Freelon. Retrieved February 17, 2022 from http://dfreelon.org/utils/recalfront/recal3/
[23] Gesellschaft für Informatik. 2022. *Startseite - Gesellschaft für Informatik e.V.* Gesellschaft für Informatik e.V. Retrieved February 18, 2022 from https://gi.de/
[24] Bundeszentrale für politische Bildung. 2020. *Stereotypisierungen von Jung und Alt in der Corona-Pandemie*. Bundeszentrale für politische Bildung. Retrieved February 17, 2022 from https://www.bpb.de/shop/zeitschriften/apuz/generationen-2020/324487/stereotypisierungen-von-jung-und-alt-in-der-corona-pandemie/#footnote-target-14
[25] Eva Ganglbauer, Geraldine Fitzpatrick, and Rob Comber. 2013. Negotiating Food Waste: Using a Practice Lens to Inform Design. *ACM Trans. Comput.-Hum. Interact.* 20, 2, Article 11 (may 2013), 25 pages. https://doi.org/10.1145/2463579.2463582
[26] GitHub. 2020. *App closing immediately on start - Issue 1053*. GitHub. Retrieved February 17, 2022 from https://github.com/corona-warn-app/cwa-app-android/issues/1053
[27] GitHub. 2020. *Error Reason: 2001; App does not work anymore - Issue 968*. GitHub. Retrieved February 17, 2022 from https://github.com/corona-warn-app/cwa-app-android/issues/968
[28] GitHub. 2020. *[INFO] URSACHE: 9002, Etwas ist schiefgelaufen. Timeout - Issue 998*. GitHub. Retrieved February 17, 2022 from https://github.com/corona-warn-app/cwa-app-android/issues/998
[29] GitHub. 2020. *Release 1.1.2*. GitHub. Retrieved January 28, 2022 from https://github.com/corona-warn-app/cwa-app-ios/releases/tag/v1.1.2
[30] GitHub. 2020. *Releases - Corona Warn App*. GitHub. Retrieved February 17, 2022 from https://github.com/corona-warn-app/cwa-app-android/releases
[31] Handelsblatt. 2020. *Corona-Warn-App: Bundesregierung zahlte 7,5 Millionen Euro für Werbung*. Handelsblatt. Retrieved February 17, 2022 from https://www.handelsblatt.com/technik/it-internet/werbekampagne-corona-warn-app-bundesregierung-zahlte-7-5-millionen-euro-fuer-werbung/26021070.html
[32] Maximilian Häring, Eva Gerlitz, Christian Tiefenau, Matthew Smith, Dominik Wermke, Sascha Fahl, and Yasemin Acar. 2021. Never ever or no matter what: Investigating Adoption Intentions and Misconceptions about the Corona-Warn-App in Germany. In *Seventeenth Symposium on Usable Privacy and Security (SOUPS 2021)*. USENIX Association, online, 77–98. https://www.usenix.org/conference/soups2021/presentation/acar
[33] Robert Hinch, Will Probert, Anel Nurtay, Michelle Kendall, Chris Wymant, Matthew Hall, Katrina Lythgoe, Ana Bulas Cruz, Lele Zhao, Andrea Stewart, et al. 2020. Effective configurations of a digital contact tracing app: a report to NHSX. *Retrieved July* 23 (2020), 2020.
[34] Kai T Horstmann, Susanne Buecker, Julia Krasko, Sarah Kritzler, and Sophia Terwiel. 2021. Who does or does not use the 'Corona-Warn-App'and why? *European Journal of Public Health* 31, 1 (2021), 49–51.
[35] Laszlo Horvath, Susan Banducci, and Oliver James. 2020. Citizens' Attitudes to Contact Tracing Apps. *Journal of Experimental Political Science* 9 (2020), 1–13. https://doi.org/10.1017/XPS.2020.30
[36] Jack Jamieson, Daniel A. Epstein, Yunan Chen, and Naomi Yamashita. 2022. Unpacking Intention and Behavior: Explaining Contact Tracing App Adoption and Hesitancy in the United States. In *CHI Conference on Human Factors in Computing Systems* (2022) *(CHI '22)*. Association for Computing Machinery, New York, NY, USA, Article 79, 14 pages. https://doi.org/10.1145/3491102.3501963
[37] Genia Kostka and Sabrina Habich-Sobiegalla. 2020. In Times of Crisis: Public Perceptions Towards COVID-19 Contact Tracing Apps in China, Germany and the US. *SSRN Electronic Journal* 0 (2020), 28 pages. https://doi.org/10.2139/ssrn.3693783
[38] Anastasia Kozyreva, Philipp Lorenz-Spreen, Stephan Lewandowsky, Paul M. Garrett, Stefan M. Herzog, Thorsten Pachur, and Ralph Hertwig. 2021. Psychological Factors Shaping Public Responses to COVID-19 Digital Contact Tracing Technologies in Germany. *Scientific Reports* 11, 1 (2021), 18716. Issue 1. https://doi.org/10.1038/s41598-021-98249-5
[39] Oksana Kulyk, Lauren Britton-Steele, Elda Paja, Melanie Duckert, and Louise Barkhuus. 2022. #34;You Have Been in Close Contact with a Person Infected with COVID-19 and You May Have Been Infected#34;: Understanding Privacy Concerns, Trust and Adoption in Mobile COVID-19 Tracing Across Four Countries. *Proc. ACM Hum.-Comput. Interact.* 6, MHCI, Article 204 (sep 2022), 27 pages. https://doi.org/10.1145/3546739
[40] Xi Lu, Tera L. Reynolds, Eunkyung Jo, Hwajung Hong, Xinru Page, Yunan Chen, and Daniel A. Epstein. 2021. Comparing Perspectives around Human and Technology Support for Contact Tracing. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems* (2021) *(CHI '21)*. Association for Computing Machinery, New York, NY, USA, Article 200, 15 pages. https://doi.org/10.1145/3411764.3445669
[41] Yao Lyu and John M. Carroll. 2022. Cultural Influences on Chinese Citizens' Adoption of Digital Contact Tracing: A Human Infrastructure Perspective. In *Proceedings of the 2022 CHI Conference on Human Factors in Computing Systems* (New Orleans, LA, USA) *(CHI '22)*. Association for Computing Machinery, New York, NY, USA, Article 252, 17 pages. https://doi.org/10.1145/3491102.3517572
[42] Yannic Meier, Judith Meinert, and Nicole C. Krämer. 2021. Investigating Factors That Affect the Adoption of COVID-19 Contact-Tracing Apps: A Privacy Calculus Perspective. *Technology, Mind, and Behavior* 2, 3 (2021), 1–10. https://doi.org/10.1037/tmb0000040
[43] Simon Munzert, Peter Selb, Anita Gohdes, Lukas F. Stoetzer, and Will Lowe. 2021. Tracking and Promoting the Usage of a COVID-19 Contact Tracing App. *Nature Human Behaviour* 5, 2 (2021), 247–255. Issue 2. https://doi.org/10.1038/s41562-020-01044-x
[44] Heise Online. 2020. *Zero Rating: Mobilfunk-Provider berechnen keinen Traffic für Corona-Warn-App*. Heise Medien GmbH & Co. KG. Retrieved February 17, 2022 from https://www.heise.de/news/Zero-Rating-Mobilfunk-Provider-berechnen-keinen-Traffic-fuer-Corona-Warn-App-4785202.html
[45] Cliodhna O'Connor and Helene Joffe. 2020. Intercoder Reliability in Qualitative Research: Debates and Practical Guidelines. *International Journal of Qualitative Methods* 19 (2020), 1609406919899220. https://doi.org/10.1177/1609406919899220
[46] Charlie Pinder, Jo Vermeulen, Benjamin R. Cowan, and Russell Beale. 2018. Digital Behaviour Change Interventions to Break and Form Habits. *ACM Trans. Comput.-Hum. Interact.* 25, 3, Article 15 (jun 2018), 66 pages. https://doi.org/10.1145/3196830
[47] Qualtrics. 2022. . Qualtrics. Retrieved February 17, 2022 from qualtrics.com
[48] John S. Seberger and Sameer Patil. 2021. Us and Them (and It): Social Orientation, Privacy Concerns, and Expected Use of Pandemic-Tracking Apps in the United States. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems* (Yokohama, Japan) *(CHI '21)*. Association for Computing Machinery, New York, NY, USA, Article 65, 19 pages. https://doi.org/10.1145/3411764.3445485
[49] Paschal Sheeran and Thomas L. Webb. 2016. The Intention-Behavior Gap: The Intention-Behavior Gap. *Social and Personality Psychology Compass* 10, 9 (2016), 503–518. https://doi.org/10.1111/spc3.12265
[50] Lucy Simko, Jack L. Chang, Maggie Jiang, Ryan Calo, Franziska Roesner, and Tadayoshi Kohno. 2020. COVID-19 Contact Tracing and Privacy: A Longitudinal Study of Public Opinion. *arXiv preprint arXiv:2012.01553* abs/2012.01553 (2020), 37 pages. https://doi.org/10.48550/arXiv.2012.01553
[51] Spiegel. 2020. *So erkennen Sie, ob Ihre Corona-App richtig funktioniert*. DER SPIEGEL GmbH & Co. KG. Retrieved September 6, 2022 from https://www.spiegel.de/netzwelt/corona-warn-app-wann-die-app-auf-android-und-ios-vollstaendig-funktioniert-a-0088dfd8-d6b5-41d5-8855-513371dcb71f
[52] Statista. 2021. *Anzahl der Downloads der Corona-Warn-App über den Apple App Store und den Google Play Store (kumuliert) in Deutschland von Juni 2020 bis Dezember 2022*. Statista. Retrieved December 12, 2022 from https://de.statista.com/statistik/daten/studie/1125951/umfrage/downloads-der-corona-warn-app/
[53] Statista. 2021. *Anzahl der Smartphone-Nutzer* in Deutschland in den Jahren 2009 bis 2021*. Statista. Retrieved February 17, 2022 from https://de.statista.com/statistik/daten/studie/198959/umfrage/anzahl-der-smartphonenutzer-in-deutschland-seit-2010/
[54] Hanns Seidel Stiftung. 2020. *Zur Dynamik der Corona-Demonstrationen*. Hanns-Seidel-Stiftung e.V. Retrieved February 18, 2022 from https://www.hss.de/

publikationen/zur-dynamik-der-corona-demonstrationen-pub1703/
[55] Tagesschau. 2020. *Corona-Tracing: Bundesregierung denkt bei App um.* Norddeutscher Rundfunk. Retrieved January 28, 2021 from https://www.tagesschau.de/inland/coronavirus-app-107.html
[56] Tagesschau. 2020. *Corona-Warn-App: iPhone-Lücke war seit Wochen bekannt.* Norddeutscher Rundfunk. Retrieved February 17, 2022 from https://www.tagesschau.de/investigativ/corona-warn-app-121.html
[57] Tagesschau. 2020. *Lücken bei Kontaktüberprüfung: Corona-App funktioniert auf iPhones fehlerhaft.* Norddeutscher Rundfunk. Retrieved February 17, 2022 from https://www.tagesschau.de/investigativ/corona-warn-app-113.html
[58] Tagesschau. 2020. *Pläne von Minister Spahn - Kritik an Corona-App wächst.* Norddeutscher Rundfunk. Retrieved February 17, 2022 from https://www.tagesschau.de/inland/corona-app-spahn-101.html
[59] Tagesschau. 2020. tagesschau 20:00 Uhr, 25.07.2020. Video. Retrieved September 6, 2022 from https://www.youtube.com/watch?v=7zqLTA-1nHk
[60] Technologyreview. 2020. *No, coronavirus apps don't need 60% adoption to be effective.* MIT Technologyreview. Retrieved February 17, 2022 from https://www.technologyreview.com/2020/06/05/1002775/covid-apps-effective-at-less-than-60-percent-download/
[61] Rae Thomas, Zoe A Michaleff, Hannah Greenwood, Eman Abukmail, and Paul Glasziou. 2020. Concerns and Misconceptions About the Australian Government's COVIDSafe App: Cross-Sectional Survey Study. *JMIR Public Health and Surveillance* 6, 4 (2020), e23081. https://doi.org/10.2196/23081
[62] Samuel Tomczyk, Simon Barth, Silke Schmidt, and Holger Muehlan. 2021. Utilizing Health Behavior Change and Technology Acceptance Models to Predict the Adoption of COVID-19 Contact Tracing Apps: Cross-sectional Survey Study. *Journal of Medical Internet Research* 23, 5 (2021), e25447. https://doi.org/10.2196/25447
[63] Presse und Informationsamt der Bundesregierung. 2022. *Corona-Warn-App: der Baukasten für Unterstützerinnen und Unterstützer.* Bundesregierung. Retrieved January 23, 2023 from https://styleguide.bundesregierung.de/sg-de/basiselemente/programmmarken/corona-warn-app
[64] UNESCO. 2011. *UNESCO | International Standard Classification of Education.* UNESCO. Retrieved February 08, 2023 from http://uis.unesco.org/en/files/international-standard-classification-education-isced-2011-en-pdf
[65] Christine Utz, Steffen Becker, Theodor Schnitzler, Florian M. Farke, Franziska Herbert, Leonie Schaewitz, Martin Degeling, and Markus Dürmuth. 2021. Apps Against the Spread: Privacy Implications and User Acceptance of COVID-19-Related Smartphone Apps on Three Continents. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems* (Yokohama, Japan) *(CHI '21)*. Association for Computing Machinery, New York, NY, USA, Article 70, 22 pages. https://doi.org/10.1145/3411764.3445517
[66] Verbraucherschutz. 2020. *Facebook & WhatsApp: Kettenbrief zu STOPCOVID-App – Stimmt das?* Verbraucherschutz. Retrieved February 17, 2022 from https://www.verbraucherschutz.com/warnungsticker/facebook-whatsapp-kettenbrief-zu-stopcovid-app-stimmt-das/
[67] My Villius Zetterholm, Yanqing Lin, and Päivi Jokela. 2021. Digital Contact Tracing Applications during COVID-19: A Scoping Review about Public Acceptance. *Informatics* 8, 3 (2021), 48. https://doi.org/10.3390/informatics8030048
[68] Simon N. Williams, Christopher J. Armitage, Tova Tampe, and Kimberly Dienes. 2021. Public Attitudes towards COVID-19 Contact Tracing Apps: A UK-based Focus Group Study. *Health Expectations* 24, 2 (2021), 377–385. https://doi.org/10.1111/hex.13179
[69] ZDF. 2020. *Chaos Computer Club lobt deutsche Corona-App.* ZDF. Retrieved April 24, 2022 from https://web.archive.org/web/20211222145023/https://www.zdf.de/nachrichten/politik/corona-app-launch-100.html
[70] ZDF. 2020. *Keine Hintergrundaktualisierung-Einstellung bei Warn-App: Was man wissen muss.* ZDF. Retrieved April 24, 2022 from https://web.archive.org/web/20211113120146/https://www.zdf.de/nachrichten/digitales/coronavirus-warnapp-fehlfunktion-android-100.html
[71] ZDF. 2020. *Probleme bei der Nutzung-Die vielen Fehlermeldungen der Corona-App.* ZDF. Retrieved April 24, 2022 from https://web.archive.org/web/20210323025851/https://www.zdf.de/nachrichten/politik/corona-app-fehlermeldungen-102.html
[72] Zusammengegencorona. 2022. *Fake-News rund um das Coronavirus.* Bundesministerium für Gesundheit. Retrieved February 17, 2022 from https://www.zusammengegencorona.de/informieren/alltag-und-reisen/fake-news-rund-um-das-coronavirus/

Code	% in data set (installation status per code in %): cwa_int (✓, unclear, ×)	cwa_beh (✓, unclear, ×)	ICR_int	ICR_beh	Example
C1: Pandemic control and health [34, 38, 42, 65]	**33.6** (98, 1.6, 0.4)	**34.8** (90.4, 0.3, 9.3)	0.95	0.92	"Avoiding another lockdown", "To combat the pandemic", "Solidarity"
C2: Technical[6, 34, 43, 65]	**2.8** (19.0, 19.0, 61.9)	**12.2** (1.0, 0.0, 99.0)			
Phone usage/Inconvenient	1.6 (16.7, 25, 58.3)	5.7 (0, 0, 100)	0.89	0.97	"I do not want to enable Bluetooth", "Rarely have my smartphone with me"
Not supported	0.1 (100, 0, 0)	4.5 (0, 0, 100)	undef*	0.85	"It does not work with my phone"
Technical side effects	0.9 (14.3, 14.3, 71.4)	1.8 (6.7, 0, 93.3)	1	1	"High data consumption", "Bluetooth draws battery"
Technical general	0.1 (0, 0, 100)	0.2 (0, 0, 100)	undef*	undef*	"Bluetooth"
Not sure if allowed	-	0.1 (0, 0, 100)	-	undef*	"Since it's a company phone, I need to clarify first if I'm allowed to install the app."
C3: Unnecessary [34, 65]	**6.4** (8.7, 26.1, 65.2)	**12.0** (2, 0, 98)			
Personal behavior	1.6 (16.7, 33.3, 50)	6.1 (3.9, 0, 96.1)	undef*	0.92	"Since I spend almost all my time at home"
Unnecessary general	1.6 (8.3, 16.7, 75)	3.7 (0, 0, 100)	<0.5*	0.82	"I do not need it", "Because I already know everything about Corona"
State of the pandemic	1.6 (8.3, 33.3, 58.3)	1.4 (0, 0, 100)	1	0.89	"They should have done something like this right at the outbreak of Covid, now it's not worth it."
Don't Care	1.5 (0, 9.1, 90.9)	0.8 (0, 0, 100)	0.92	<0.5*	"I Do not consider the threat of Corona so extreme that it requires an app"
Other	0.1 (0, 100, 0)	-	undef*	-	"I think it would be better to be warned before you meet an infected person."
C4: Does it work [6, 34, 38, 43, 65]	**3.9** (17.2, 51.7, 31)	**9.2** (2.7, 0, 97.3)			
Does it work general	1.9 (28.6, 64.3, 7.1)	4.8 (0, 0, 100)	0.9	0.91	"I doubt the functionality", "Does it really do that much?"
Malfunctions	1.1 (0, 37.5, 62.5)	2.4 (0, 0, 100)	1	1	"Did not work properly and too often constantly loaded or announced updates!"
Usage	0.9 (14.3, 42.9, 42.9)	2 (11.8, 0, 88.2)	<0.5*	0.86	"I do not think it makes sense as long as a large majority does not use this app"
C5: Distrust/Abuse [6, 43, 65]	**14.2** (2, 25.3, 72.7)	**8.8** (0, 1.4, 98.6)			
(Government) Surveillance	7.9 (1.7, 16.9, 81.4)	3.9 (0, 3, 97)	0.94	0.95	"I see no added value to install spyware.", "Big brother"
Distrust general	1.3 (10, 50, 40)	2.2 (0, 0, 100)	1	0.67*	"No trust in the parties involved"
Autonomy	3.9 (0, 37.9, 62.1)	1.4 (0, 0, 100)	0.91	0.86	"Too much statehood, too much control.", "Violation of basic rights"
Disinformation	1.1 (0, 37.5, 62.5)	0.7 (0, 0, 100)	0.66*	<0.5*	"This app could also be used for other things.",
Negative Reviews	-	0.6 (0, 0, 100)	-	undef*	"Didn't work that well with acquaintances,"
C6: Other	**6.0** (13.3, 48.9, 37.8)	**8.7** (21.9, 0.0, 78.1)			
Don't want	1.6 (0, 8.3, 91.7)	3 (0, 0, 100)	1	0.72*	"Lack of interest"
Lack of information[34, 43, 65]	3.8 (3.6, 75, 21.4)	2.2 (0, 0, 100)	<0.5*	0.88	"I need more information to decide"
Testing	0.7 (100, 0, 0)	1.8 (60, 0, 40)	undef*	1	"Just wanted to test it"
Recommended by others	-	1.1 (77.8, 0, 22.2)	-	1	"Colleagues said it would be helpful"
No time yet/forgot [34]	-	1 (0, 0, 100)		undef*	"Have always put it off until now"
C7: Privacy [3, 6, 20, 34, 38, 43, 62, 65]	**14.5** (4.6, 46.3, 49.1)	**5.5** (2.2, 0, 97.8)			
Privacy negative	14.5 (4.6, 46.3, 49.1)	5.4 (0, 0, 100)	0.94	0.86	"Privacy is violated and everyone knows where I am currently staying"
Privacy positive	-	0.1 (100, 0, 0)	-	undef*	"The app is privacy compliant and shares only anonymized data (Bluetooth ID)"
C8: Psychological+Societal [34, 65]	**5.4** (62.5, 7.5, 30)	**1.1** (44.4, 0, 55.6)			
Negative feelings	1.9 (7.1, 14.3, 78.6)	0.4 (0, 0, 100)	0.75*	undef*	"Is creepy to me"
Positive feelings	2.4 (100, 0, 0)	0.4 (33.3, 0, 66.7)	0.82	0.66*	"To make me feel safer", "It would calm me down when I am outside"
(Not) mandatory	0.4 (33.3, 33.3, 33.3)	0.2 (100, 0, 0)	undef*	1	"My company requested it"
Trust (positive) [3, 42]	0.7 (100, 0, 0)	0.1 (100, 0, 0)	1	undef*	"Sounds credible and developers are known"
C9: Security [3, 65]	**1.6** (8.3, 58.3, 33.3)	**0.6** (0, 0, 100)			
Security negative	1.5 (0, 63.6, 36.4)	0.6 (0.0, 0.0, 100.0)	<0.5*	1	"The security is questionable", "Cybercrime"
Security positive	0.1 (100, 0, 0)	-	undef*	-	"I consider it secure."
C10: Unhelpful	**19.8** (56.5, 33.3, 10.2)	**15.9** (54.1, 3.0, 42.9)			
Safety/Security	3.4 (96, 4, 0)	4.8 (87.5, 2.5, 10)	0.68*	0.78*	"Safety"/"Security" (Same word in German)
Generic positive	4.2 (100, 0, 0)	3.7 (83.9, 0, 16.1)	0.87	0.83	"I am convinced of the concept of the app", " I like it so much"
No answer	2.8 (38.1, 47.6, 14.3)	2.3 (15.8, 10.5, 73.7)	<0.5*	0.75*	"My opinion", "No statement"
Unclear	3.5 (50, 30.8, 19.2)	2.3 (42.1, 0, 57.9)	<0.5*	0.54*	"The panic of my partner", "Information"
Don't know	4.3 (18.8, 75, 6.2)	1.9 (0, 6.2, 93.8)	0.54*	0.75*	"Undecided", "Not thought about it yet"
Uncertain/Insecure	0.9 (14.3, 85.7, 0)	0.8 (0, 0, 100)	<0.5*	1	"Uncertain"/"Insecure" (Same word in German)
Generic negative	0.7 (0, 0, 100)	0.1 (0, 0, 100)	<0.5*	0.5*	"I do not like it", "Antipathy"

Table 2: Full coding table of reasons for the installation status. Codes are sorted by number of appearances. Numbers for high-level code are the sums of sub codes, if any exist. If ICR (Inter-coder reliability, Krippendorff's alpha) was less than 0.8, it is marked with "*". There were codes not occuring in the subset of documents used to calculate the ICR. These codes are marked with "undef" and also "*" All documents containing one of those codes, marked with "*", were discussed among the authors. The references mark related work that found similar reasons.

		Overall		Age										Education							
				18-24		25-34		35-49		50-64		>=65		Not discl.		ISCED 0-2		ISCED 3-4		ISCED 5-8	
	CWA-Study	int	beh	int	beh	int	beh	int	beh	int	beh	int	beh	int	beh	int	beh	int	beh	int	beh
	Total	**744**	**837**	**180**	**87**	**106**	**140**	**178**	**212**	**199**	**228**	**81**	**170**	**17**	**9**	**51**	**58**	**373**	**491**	**303**	**279**
	Installed (Intention vs. Behavior)	50.1	42.8	45.0	42.5	40.6	37.9	50.6	47.2	51.3	38.2	69.1	47.1	35.3	33.3	37.3	31.0	46.4	38.5	57.4	52.7
Code	C1: Pandemic control and health	33.6	34.9	26.1	40.2	20.8	32.1	36.5	35.8	36.7	28.5	53.1	41.2	23.5	22.2	21.6	25.9	30.8	31.8	39.6	42.3
	C2: Technical	2.8	12.2	3.3	12.6	0.9	7.9	1.7	8.0	4.0	11.4	3.7	21.8	5.9	22.2	-	3.4	2.4	13.4	3.6	11.5
	C3: Unnecessary	6.2	11.8	10.0	10.3	5.7	13.6	3.9	11.8	6.5	11.8	2.5	10.6	17.6	11.1	3.9	15.5	8.0	12.0	3.6	10.4
	C4: Does it work	3.9	8.9	5.0	4.6	0.9	12.9	4.5	8.5	3.0	10.5	6.2	5.9	5.9	-	3.9	10.3	4.8	8.8	2.6	9.0
	C5: Distrust/Abuse	13.3	8.6	11.7	9.2	17.9	9.3	11.8	7.5	15.6	11.0	8.6	5.9	11.8	11.1	13.7	13.8	13.7	9.6	12.9	5.7
	C6: Other	6.1	8.8	7.2	14.9	9.4	7.9	6.7	10.8	4.5	7.9	1.2	4.7	11.8	11.1	7.8	15.5	6.7	9.0	4.6	6.8
	C7: Privacy	14.6	5.5	15.6	5.7	23.6	7.1	15.2	6.1	13.1	6.6	2.5	1.8	5.9	22.2	13.7	12.1	15.8	5.3	13.5	3.9
	C8: Psychological/Societal	5.4	1.1	7.2	-	3.8	2.1	4.5	0.9	5.5	0.9	4.9	1.2	5.9	-	7.8	1.7	5.9	1.0	4.3	1.1
	C9: Security	1.6	0.6	2.8	-	1.9	0.7	1.1	0.9	1.5	0.9	-	-	-	-	3.9	-	1.6	0.8	1.3	0.4
	C10: Unhelpful	19.7	15.6	22.8	6.9	25.5	16.4	19.1	18.4	14.1	18.9	21.0	12.9	29.4	22.2	27.5	12.1	19.0	16.7	18.8	15.1
	Total	**657**	**826**	**148**	**85**	**88**	**140**	**160**	**210**	**184**	**224**	**77**	**167**	**14**	**9**	**38**	**54**	**327**	**485**	**278**	**278**
Attributes	**Correct attributes**																				
	AT1: USES BLUETOOTH	43.7	65.4	38.5	63.5	28.4	62.1	49.4	68.6	47.8	66.1	48.1	64.1	42.9	55.6	28.9	63.0	41.0	62.9	48.6	70.5
	AT2: DETECTS NEARBY USERS	52.5	53.5	51.4	56.5	50.0	50.0	47.5	56.7	57.6	54.9	55.8	48.5	42.9	55.6	39.5	46.3	51.7	51.8	55.8	57.6
	AT3: SHARES TEMPORARY IDS	29.8	27.0	39.9	36.5	37.5	35.0	30.0	29.0	23.9	25.0	15.6	15.0	28.6	22.2	26.3	25.9	32.4	25.6	27.3	29.5
	AT4: INFORMS ME IF CONTACT INFECTED	73.7	70.5	80.4	84.7	75.0	79.3	68.1	74.3	75.5	63.4	66.2	60.5	42.9	77.8	57.9	59.3	74.9	70.3	75.9	72.7
	AT5: INFORMS MY CONTACTS	70.5	78.0	70.3	82.4	64.8	82.1	66.9	78.6	73.4	72.3	77.9	79.0	50.0	77.8	55.3	72.2	72.2	77.3	71.6	80.2
	AT6: DATA TRANSMISSION ONLY AFTER CONFIRMATION	44.4	37.8	60.1	56.5	54.5	44.3	38.8	32.4	36.4	35.7	33.8	32.3	42.9	44.4	42.1	38.9	45.6	37.5	43.5	37.8
	Incorrect attributes																				
	AF1: CAN DONATE HEALTH DATA	35.0	22.1	41.2	32.9	36.4	26.4	33.8	24.3	33.7	17.9	26.0	15.6	57.1	22.2	28.9	35.2	36.1	22.9	33.1	18.0
	AF2: GOVERNMENT CAN TRACK ME	27.2	11.5	33.8	15.3	36.4	10.7	25.6	10.0	19.0	13.4	27.3	9.6	28.6	-	44.7	25.9	26.9	11.1	25.2	9.7
	AF3: GOVERNMENT SEES DISTANCE VIOLATION	20.6	7.2	21.6	9.4	23.9	6.4	23.1	6.2	16.8	8.5	19.5	6.6	7.1	-	26.3	13.0	20.5	7.4	20.9	6.1
	AF4: MANDATORY USAGE	7.2	0.9	11.5	1.2	13.6	0.7	7.5	1.9	2.2	-	2.6	0.6	14.3	11.1	13.2	-	7.6	0.4	5.4	1.4
	AF5: SHARE PHONE CONTACTS WITH GOVERNMENT	15.7	6.1	22.3	9.4	20.5	3.6	15.0	5.7	12.0	5.8	9.1	7.2	35.7	11.1	26.3	14.8	16.5	4.7	12.6	6.5
	AF6: SHOWS NEGATIVE INFECTION STATE	32.1	31.2	39.2	34.1	28.4	31.4	27.5	29.0	31.5	31.2	33.8	31.7	50.0	33.3	31.6	40.7	32.4	32.6	30.9	26.6
	AF7: SHARES FITNESS DATA	5.8	1.3	4.7	3.5	10.2	-	6.2	2.9	4.9	0.4	3.9	0.6	21.4	-	10.5	-	4.0	1.2	6.5	1.8
	AF8: SHARES MOTION PROFILE	41.8	24.1	47.3	23.5	47.7	22.9	40.0	21.9	38.6	26.3	36.4	25.7	42.9	11.1	47.4	31.5	42.5	24.7	40.3	22.3
	NONE (GENERAL)	0.3	0.5	0.7	-	-	-	-	1.0	0.5	0.4	-	0.6	-	-	-	-	0.3	0.4	0.4	0.7
	AF9: GOVERNMENT SEES OTHERS' QUARANTINE VIOLATION	34.4	9.2	43.2	14.1	47.7	7.1	36.2	6.7	25.5	14.3	20.8	4.8	35.7	11.1	50.0	18.5	34.6	8.2	32.4	9.0
	AF10: INFORMS IF INFECTED NEARBY	57.6	55.7	62.8	60.0	58.0	50.7	51.9	46.2	57.1	58.9	59.7	64.7	57.1	55.6	57.9	66.7	59.9	57.3	54.7	50.4
	NONE (OTHER)	1.7	2.4	2.7	-	2.3	2.9	1.9	0.5	1.1	3.6	-	4.2	7.1	-	2.6	3.7	1.8	2.3	1.1	2.5
	AF11: SHARES DATA CONTINUOUSLY	35.1	21.0	42.6	18.8	43.2	19.3	36.2	21.0	30.4	20.5	22.1	24.0	28.6	33.3	42.1	24.1	36.7	22.1	33.1	18.0
	AF12: GOVERNMENT SEES MY QUARANTINE VIOLATION	35.7	9.5	48.0	16.5	44.3	6.4	38.1	9.0	25.5	11.6	22.1	6.0	42.9	-	47.4	18.5	35.8	8.7	33.8	9.4
	NONE (SELF)	2.3	2.6	0.7	-	1.1	3.6	2.5	1.4	4.3	4.0	1.3	2.4	-	-	2.6	3.7	1.5	2.5	3.2	2.5
	No truth value assignable																				
	AN1: RESTRICTS BASIC RIGHTS	20.0	6.4	24.3	8.2	21.6	7.9	21.2	6.2	18.5	7.1	11.7	3.6	14.3	-	34.2	11.1	19.9	6.8	18.7	5.0
	AN2: HELPS WITH TESTING DECISION	41.4	28.6	52.7	43.5	37.5	27.9	33.1	27.1	39.1	25.4	46.8	28.1	42.9	22.2	34.2	22.2	41.0	29.3	42.8	29.1
	AN3:FIGHTS DISEASE SPREAD	69.9	77.4	67.6	77.6	58.0	78.6	68.1	78.1	73.4	72.3	83.1	82.0	57.1	66.7	52.6	70.4	70.6	76.1	71.9	81.3
	AN4: USES LOCATION SERVICES	54.7	35.6	64.2	47.1	62.5	40.0	53.1	34.8	45.1	35.3	53.2	28.1	57.1	11.1	60.5	46.3	54.7	34.0	53.6	37.4
	AN5: THREATS PRIVACY	27.4	11.4	36.5	11.8	35.2	15.7	26.2	10.0	23.9	13.4	11.7	6.6	50.0	11.1	42.1	18.5	29.4	10.9	21.9	10.8
	AN6: DON'T KNOW (GENERAL)	4.3	2.2	4.1	2.4	3.4	2.1	5.6	2.4	4.3	3.1	2.6	0.6	14.3	11.1	7.9	5.6	3.7	2.1	4.0	1.4
	AN7: DON'T KNOW (OTHER)	6.0	3.6	4.7	3.5	4.5	2.1	7.5	3.3	6.0	6.7	6.5	1.2	14.3	22.2	10.5	9.3	6.4	3.7	4.3	1.8
	AN8: DON'T KNOW (SELF)	9.8	7.4	8.1	5.9	4.5	6.4	13.8	9.0	8.7	8.9	13.0	5.4	35.7	22.2	13.2	13.0	10.1	7.8	7.6	5.4
	Basic Knowledge Score	10.8	13.6	14.3	17.9	8.0	18.1	14.4	18.1	12.5	12.9	7.9	4.2	7.1	11.1	8.1	15.1	12.2	11.8	13.0	17.3

Table 3: Table of occurred codes and marked attributes split by the socio-demographic groups "age" and "education". Numbers, except totals, in %.

		Gender				Income													
		Female		Male		Not discl.		<1300€		1300-1700€		1700-2600€		2600-3600€		3600-5000€		>5000€	
	CWA-Study	int	beh	int	beh	int	beh	int	beh	int	beh	int	beh	int	beh	int	beh	int	beh
	Total	**416**	**453**	**322**	**382**	**79**	**32**	**136**	**140**	**100**	**63**	**155**	**187**	**124**	**170**	**104**	**171**	**46**	**74**
	Installed (Intention vs. Behavior)	47.1	36.6	54.7	49.5	41.8	34.4	41.2	30.0	51.0	36.5	52.3	39.0	54.0	46.5	50.0	52.0	69.6	54.1
Code	C1: Pandemic control and health	30.0	30.9	38.8	39.0	25.3	34.4	26.5	26.4	28.0	30.2	35.5	33.2	40.3	32.9	36.5	43.3	50.0	43.2
	C2: Technical	2.9	13.5	2.8	10.7	1.3	12.5	5.1	15.7	3.0	14.3	3.2	13.9	2.4	10.0	-	9.9	4.3	9.5
	C3: Unnecessary	6.5	13.7	5.9	9.4	6.3	9.4	8.1	16.4	4.0	11.1	7.1	13.4	7.3	5.9	3.8	10.5	4.3	16.2
	C4: Does it work	4.6	9.7	3.1	7.9	3.8	15.6	5.1	7.9	2.0	6.3	3.9	9.1	4.8	8.8	3.8	8.8	2.2	9.5
	C5: Distrust/Abuse	13.5	8.8	12.1	8.4	20.3	6.2	14.7	10.0	11.0	15.9	12.3	10.2	11.3	7.1	14.4	7.0	8.7	4.1
	C6: Other	6.2	7.9	5.6	9.7	7.6	3.1	6.6	9.3	4.0	7.9	7.1	10.2	4.0	10.0	7.7	8.8	4.3	4.1
	C7: Privacy	15.4	5.3	13.7	5.8	12.7	6.2	15.4	4.3	14.0	3.2	14.2	6.4	18.5	8.8	12.5	3.5	10.9	4.1
	C8: Psychological/Societal	6.5	1.8	3.7	0.3	7.6	-	4.4	0.7	6.0	-	5.8	1.6	5.6	2.4	5.8	-	-	1.4
	C9: Security	1.4	0.4	1.9	0.8	-	-	2.2	0.7	1.0	-	0.6	0.5	2.4	0.6	2.9	0.6	2.2	1.4
	C10: Unhelpful	20.2	17.7	19.6	13.9	22.8	15.6	20.6	16.4	30.0	17.5	17.4	12.8	14.5	21.2	17.3	14.0	17.4	13.5
	Total	**359**	**446**	**294**	**378**	**71**	**30**	**112**	**136**	**85**	**62**	**139**	**186**	**109**	**169**	**98**	**169**	**43**	**74**
Attributes	**Correct attributes**																		
	AT1: USES BLUETOOTH	37.0	58.1	51.7	73.8	45.1	56.7	48.2	61.8	36.5	50.0	43.9	68.3	41.3	68.6	36.7	70.4	62.8	62.2
	AT2: DETECTS NEARBY USERS	51.0	50.4	54.8	56.6	57.7	60.0	52.7	50.7	45.9	33.9	56.1	55.9	54.1	49.7	42.9	59.2	62.8	60.8
	AT3: SHARES TEMPORARY IDS	29.0	23.3	31.0	31.0	36.6	30.0	37.5	24.3	27.1	22.6	27.3	28.5	26.6	23.7	23.5	27.2	34.9	36.5
	AT4: INFORMS ME IF CONTACT INFECTED	74.9	71.1	72.1	69.6	71.8	63.3	72.3	59.6	65.9	69.4	74.1	73.1	72.5	69.8	77.6	71.6	88.4	86.5
	AT5: INFORMS MY CONTACTS	72.1	80.0	68.7	75.4	70.4	70.0	73.2	71.3	62.4	71.0	70.5	80.6	68.8	78.1	70.4	83.4	83.7	79.7
	AT6: DATA TRANSMISSION ONLY AFTER CONFIRMATION	50.7	40.4	36.7	34.4	47.9	23.3	44.6	36.0	44.7	41.9	46.8	38.7	37.6	36.1	42.9	40.2	51.2	39.2
	Incorrect attributes																		
	AF1: CAN DONATE HEALTH DATA	36.2	25.1	33.7	18.3	42.3	13.3	25.0	25.0	29.4	24.2	39.6	24.7	33.9	24.9	35.7	18.9	44.2	12.2
	AF2: GOVERNMENT CAN TRACK ME	28.7	13.2	25.9	9.3	32.4	10.0	35.7	15.4	25.9	14.5	33.1	11.8	20.2	14.2	23.5	6.5	7.0	6.8
	AF3: GOVERNMENT SEES DISTANCE VIOLATION	21.4	7.8	20.1	6.3	22.5	6.7	23.2	11.0	22.4	8.1	20.1	8.1	21.1	8.9	15.3	3.6	20.9	2.7
	AF4: MANDATORY USAGE	6.7	0.4	7.8	1.3	12.7	-	6.2	-	8.2	-	6.5	1.6	5.5	0.6	7.1	1.2	4.7	1.4
	AF5: SHARE PHONE CONTACTS WITH GOVERNMENT	17.3	6.7	14.3	5.3	21.1	6.7	17.9	8.8	15.3	9.7	20.9	6.5	12.8	6.5	11.2	2.4	4.7	4.1
	AF6: SHOWS NEGATIVE INFECTION STATE	31.2	32.1	33.3	29.6	33.8	40.0	31.2	33.8	37.6	45.2	36.0	31.7	33.0	24.3	23.5	29.0	25.6	29.7
	AF7: SHARES FITNESS DATA	5.3	1.3	6.5	1.3	5.6	3.3	6.2	0.7	8.2	1.6	10.1	1.6	2.8	1.8	2.0	0.6	2.3	1.4
	AF8: SHARES MOTION PROFILE	40.9	24.2	42.5	23.8	49.3	20.0	40.2	27.9	37.6	29.0	46.8	29.6	40.4	20.7	39.8	18.9	34.9	21.6
	NONE (GENERAL)	-	0.7	0.7	0.3	-	-	-	-	-	-	-	1.1	0.9	-	1.0	0.6	-	1.4
	AF9: GOVERNMENT SEES OTHERS' QUARANTINE VIOLATION	36.5	10.3	31.6	7.9	38.0	10.0	38.4	14.0	40.0	11.3	38.1	12.9	28.4	5.3	29.6	5.3	23.3	6.8
	AF10: INFORMS IF INFECTED NEARBY	61.0	57.2	53.4	53.7	47.9	46.7	64.3	61.0	57.6	64.5	60.4	59.1	62.4	54.4	50.0	52.1	51.2	43.2
	NONE (OTHER)	0.8	1.8	2.7	3.2	1.4	6.7	1.8	3.7	1.2	3.2	1.4	2.2	0.9	1.8	4.1	2.4	-	-
	AF11: SHARES DATA CONTINUOUSLY	37.0	19.7	33.3	22.5	40.8	16.7	35.7	24.3	32.9	24.2	35.3	26.9	37.6	17.8	33.7	17.8	27.9	13.5
	AF12: GOVERNMENT SEES MY QUARANTINE VIOLATION	39.3	10.5	31.3	8.2	43.7	10.0	37.5	11.8	38.8	11.3	41.7	10.8	32.1	8.9	27.6	5.9	20.9	9.5
	NONE (SELF)	1.1	2.0	3.7	3.2	1.4	-	1.8	2.9	2.4	6.5	3.6	2.2	0.9	3.0	4.1	1.2	-	2.7
	No truth value assignable																		
	AN1: RESTRICTS BASIC RIGHTS	19.8	6.5	19.7	6.3	29.6	6.7	24.1	7.4	16.5	9.7	20.1	8.6	15.6	5.9	20.4	3.6	11.6	4.1
	AN2: HELPS WITH TESTING DECISION	41.5	25.6	41.5	32.3	39.4	16.7	47.3	31.6	45.9	29.0	40.3	31.2	35.8	23.1	40.8	31.4	39.5	28.4
	AN3: FIGHTS DISEASE SPREAD	68.0	78.9	72.4	75.4	63.4	63.3	65.2	76.5	71.8	77.4	69.1	75.8	78.0	72.8	65.3	84.6	81.4	82.4
	AN4: USES LOCATION SERVICES	56.3	37.0	52.7	33.9	62.0	40.0	53.6	30.9	58.8	41.9	55.4	37.1	54.1	37.9	45.9	32.5	55.8	36.5
	AN5: THREATS PRIVACY	28.7	11.7	25.9	11.1	43.7	6.7	29.5	9.6	25.9	9.7	24.5	13.4	24.8	12.4	26.5	10.1	16.3	13.5
	AN6: DON'T KNOW (GENERAL)	5.6	2.5	2.7	1.9	7.0	6.7	4.5	2.9	4.7	1.6	4.3	2.2	2.8	3.0	4.1	0.6	2.3	1.4
	AN7: DON'T KNOW (OTHER)	6.4	4.3	5.4	2.9	9.9	6.7	7.1	6.6	8.2	1.6	6.5	3.2	2.8	4.7	5.1	1.8	-	1.4
	AN8: DON'T KNOW (SELF)	7.2	7.4	12.2	7.7	15.5	16.7	12.5	11.8	12.9	9.7	7.2	5.4	9.2	7.7	7.1	5.3	2.3	4.1
	Basic Knowledge Score	12.3	11.3	12.3	16.7	11.4	10.3	14.4	8.8	10.6	8.1	12.2	17.7	11.9	12.0	7.1	16.0	23.3	18.9

Table 4: Table of occurred codes and marked attributes split by the socio-demographic groups “gender” and “income”. Numbers, except totals, in %.