Users' Assumptions and Trust in Software vs. The Technical Reality

A Study on Contact Tracing and Secure Messaging User Experiences

Dissertation

zur

Erlangung des Doktorgrades (Dr. rer. nat.)

der

Mathematisch-Naturwissenschaftlichen Fakultät

der

Rheinischen Friedrich-Wilhelms-Universität Bonn

vorgelegt von

Maximilian Häring

aus

Krefeld

Bonn, April 2024

Angefertigt mit Genehmigung der Mathematisch-Naturwissenschaftlichen Fakultät
der Rheinischen Friedrich-Wilhelms-Universität Bonn

Gutachter/Betreuer: Prof. Dr. Matthew Smith
Gutachter: Prof. Dr. Michael Meier

Tag der Promotion: 13.09.2024
Erscheinungsjahr: 2024

Acknowledgements

Research can be a lonely journey. Thankfully, I had the opportunity to work with many great people: advisors, colleagues, co-authors, students, and friends. The work you have here in front of your eyes would not be possible without those persons.

In my academic career, I have coauthored with 26 people - I hope I do not forget someone - and I had the pleasure of working with many students. I want to take advantage of this opportunity to thank every one of them!

I want to thank my supervisor, Matthew Smith, for his endless patience and for letting me roam freely when I wanted to.

A special thanks to Chris and Eva, who have supported me in almost every one of my academic and non-academic endeavors.

I want to thank Julia for being at my side and brightening my life. She supported me on the journey in a way that cannot be measured.

At last, a very heartwarming thank you is also due to Reviewer 2 for pushing and forcing me to get better. Really, thank you!

Summary

0.1 English

Most of what increases software security and protects privacy, be it implementation or configuration, falls under the domain of security experts. But sometimes, those mechanisms need to be exposed to users who are no experts. In order to take meaningful action here, users must then be able to resolve the situation in line with their objectives. To build software that can accomplish that, it is helpful to understand how users perceive and interact with those features as well as why they do so.

Contributing to this, I studied two cases of software and researched the participants' interaction with it. I did so in three online studies with a total of 1933 participants and two lab studies with a total of 27 participants. Both apps I investigated are popular and exemplary from a technical standpoint, being open-source and focusing on privacy and security. Making them best-case objects of observation to study what users currently understand and observe their behavior.

The first software was the Corona-Warn-App (CWA), the official German digital contact tracing app. To study the CWA I conducted three online surveys. The first survey was conducted right before the app was released, and the second was conducted shortly after the release. This allowed me to measure the intention behavior gap and observe the participants' shift of reasoning, knowledge, and perception. Both surveys and contemporary related work showed that the participants had many misconceptions about how digital contact tracing worked. To investigate this further, I surveyed German participants for the third time. I found that users knew more than non-users. However, the difference was not as large as I had expected. With those surveys, I contributed to the discussion about what influenced decisions to install the CWA and what role the architecture and technical features had.

The second software I studied was the Signal app, an instant messaging application. I developed an interface for a new authentication ceremony protocol called SOAP. SOAP was developed by colleagues at ETH Zurich as part of a joint project, the "Centre for Cyber Trust" of the Werner Siemens-Stiftung. Our task at the University of Bonn was to test and improve SOAP's usability. The protocol allows users to verify that they are communicating with the intended person by letting the contact prove the possession of a social media account. The hope for SOAP was that its concept of social authentication would more closely

align with the users' already existing concepts for authentication. I conducted two lab studies investigating the interface's effectiveness in preventing insecure communications and its relation to user understanding in a whistleblower scenario. Throughout the studies, I could improve the interface so that only one in 18 failed based on SOAP. With the study, I was able to show the pitfalls of common authentication ceremonies and discuss where SOAP can improve the situation.

0.2 Deutsch

Vieles was die Softwaresicherheit erhöht oder die Privatsphäre schützt, sei es die Implementierung oder die Konfiguration, fällt in die Zuständigkeit von SicherheitsexpertInnen. Manchmal müssen die entsprechenden Mechanismen aber auch NutzerInnen, die keine ExpertenInnen sind, offengelegt werden. Um hier sinnvoll handeln zu können, müssen die NutzerInnen in der Lage sein, die Situation in Übereinstimmung mit ihren Zielen zu lösen. Um Software zu entwickeln, die dies leisten kann, ist es hilfreich zu verstehen, wie NutzerInnen diese Sicherheitsmechanismen wahrnehmen und mit ihnen interagieren.

Um das zu untersuchen, habe ich zwei Applikationen und die Interaktion der TeilnehmerInnen damit erforscht. Dazu habe ich drei Online-Studien mit insgesamt 1933 TeilnehmerInnen und zwei Laborstudien mit insgesamt 27 TeilnehmerInnen durchgeführt. Beide Apps sind populär und aus technischer Sicht vorbildlich. Sie werden als Open-Source-Software angeboten und der Schutz der Privatsphäre und der Sicherheit steht im Vordergrund. Damit sind sie optimale Beobachtungsobjekte, um zu untersuchen, was NutzerInnen derzeit verstehen und wie sie damit umgehen.

Die erste untersuchte Software war die CWA, die offizielle deutsche App zur digitalen Kontaktpersonennachverfolgung. Zur Untersuchung der CWA, habe ich drei Online-Umfragen durchgeführt. Die erste Umfrage wurde kurz vor der Veröffentlichung der App durchgeführt, die zweite kurz nach der Veröffentlichung. Auf diese Weise konnte ich den Unterschied zwischen den Absichten und dem Verhalten bezüglich der Installation messen und beobachten, wie sich die Denkweise, das Wissen und die Wahrnehmung der TeilnehmerInnen verändert. Beide Umfragen und zeitgenössische Arbeiten zeigten, dass TeilnehmerInnen viele falsche Vorstellungen darüber hatten, wie die App funktioniert. Um dies weiter zu untersuchen, habe ich eine dritte Befragung durchgeführt. Ich konnte feststellen, dass NutzerInnen der App mehr wussten als NichtnutzerInnen. Allerdings war der Unterschied kleiner als ich erwartet hatte. Mit den Ergebnisse der Umfragen trug ich zur Diskussion darüber bei, was die Entscheidung zur Installation beeinflusste und welche Rolle die Architektur und die technischen Merkmale spielten.

Die zweite Software, die ich untersucht habe, ist die Signal-App, eine Applikation für Sofortnachrichten. Ich habe eine Interface für ein neues Authentifizierungszeremonienprotokoll namens SOAP entwickelt. SOAP wurde von Kollegen der ETH Zürich im Rahmen eines gemeinsames Projektes, dem "Centre for Cyber Trust" der Werner Siemens-Stiftung, entwickelt. Unsere Aufgabe an der Universität Bonn war es SOAP bezüglich der Usability zu untersuchen und zu verbessern. Das Protokoll ermöglicht es sicherzustellen, dass man mit der gewünschten Person kommuniziert, indem man den Kontakt Zugriff zu einem frei wählbarem Social-Media-Konto nachweisen lässt. Die Hoffnung bei SOAP war, dass das Konzept besser mit den bereits bestehenden Authentifizierungskonzepten der BenutzerInnen übereinstimmen würde. In zwei Laborstudien, habe ich die Wirksamkeit des Interfaces bei der Verhinderung unsicherer Kommunikation und der Beziehung zum Verständnis der BenutzerInnen in einem Whistleblower-Szenario untersuchte. Im Laufe der Studien konnte ich die Schnittstelle so verbessern, dass nur eine von 18 Personen auf der Grundlage von SOAP fehlschlug. Außerdem konnte ich mit der Studie Fallstricke gängiger Authentifizierungszeremonien aufzeigen und diskutieren, ob SOAP die Situation verbessern kann.

Contents

Chapter 1

Introduction

Software should not only fulfill the users' intended goal, be a pleasure to work with, and be usable, but also be equipped with the best security and privacy features available. To achieve that, experts in science, security, and privacy professionals, as well as developers design and implement new security protocols, techniques, and tools that can be used to increase software security and privacy, e.g., by needing less personal data. Most of what increases security or privacy in software, be it implementation or configuration, falls under the domain of security experts. In an ideal case, they are proficient in the topic, test their software dynamically and statically, and follow best practices. Sometimes however, those mechanisms need to be exposed to users who are no experts. In order to take meaningful action here, users must then be able to resolve the situation in line with their objectives. Therefore, to build better, more usable software, it is important to know what non-experts understand and what concepts are easily picked up, e.g., because they can be related to something the users already know.

For this dissertation, I studied two cases of software and researched how the participants of the studies decided and why. More concretely, I studied why the participants decided (not) to use a software and how they behaved when confronted with a security protocol. The first software I studied was the Corona-Warn-App (CWA). The Corona-Warn-App (CWA) was the official German contact tracing app designed and used to help combat the COVID-19 pandemic from June 2020 [89] to June 2023 [79]. During the active phase of the app, the hope was that as many citizens as possible would install it, as the estimated effect on reducing the spread would be greater [107]. To reach that goal, among marketing campaigns to convey the message [96, 28], there was a focus to pick an implementation with the aim to achieve privacy and trustworthiness through transparency [83]. It was assumed and argued by public speakers [65] that the app can only succeed if it is based on the most privacy preserving technology available. Trying to increase trust through the usage and display of technical measures is not an uncommon strategy. To establish trust through transparency, the developers open sourced the code. This approach ensured that experts could inspect the code and verify that nothing malicious was implemented. In the

end, many measures were carried out to create a trustworthy app, open sourcing being just one of them. To judge whether the measures worked as expected and had a direct influence on possible users, one has to look at what knowledge reached people and what the deciding factors were to (not) use the app. In order to explore users' perceptions and handling of the app over time and its alignment with its technical reality, I conducted three online survey studies.

The second software I studied is the Signal app [181]. Signal is an instant messaging app with an "unexpected focus on privacy" [181] and recommended, e.g., by news outlets for communication of whistleblower [133, 156]. The app also tries to be trustworthy through technology, most notably through its use of End-to-end encryption (E2EE). End-to-end encryption (E2EE) provides confidentiality, meaning it enables the exchange of messages that can only be read by the intended contacts. Hence why it can enable users to communicate more freely without worrying about eavesdroppers. It is a very convenient feature for every user, especially if they want to share secrets with each other and, therefore, want to be sure that they are communicating in private. What E2EE does not offer without further action is authenticity. The app cannot know who the user is talking to. Authenticating the other party has to be done by the users themselves. This means that for E2EE to fulfill its promise of confidentiality, authenticity is necessary. Otherwise, the user can only be sure they are talking privately to someone. They just do not know who that someone is or whether there is a person-in-the-middle (PITM). At this point, the user gets in touch with the security protocol. Consequently, each effective authentication ceremony protocol and interface has to be designed not for security experts but for a broad audience. For Signal, I developed an interface for a new protocol called Social Authentication Protocol (SOAP) [134], which is intended to detect PITM attacks. The protocol allows users to verify they are communicating with the intended person by letting the contact prove the possession of a social media account. This is called social authentication. The hope for SOAP was that its concept of social authentication would more closely align with the users' already existing idea of what identities are and how authentication can work. To test whether this is the case and how it influences behavior, I conducted two lab studies investigating the interface's effectiveness in preventing insecure communications and its relation to user understanding.

Both apps, the CWA and Signal, cover two different categories (public health and private communication). Both are popular applications and are not only used by experts. Additionally, both are exemplary from a technical standpoint, being open-source and focusing on privacy and security. Making them best-case objects of observation to study what users currently understand and whether that influences their decisions.

1.1 Structure

This dissertation is structured around four user studies and is based on previous publications or work currently under review. A disclaimer at the beginning of each chapter states my contribution to these works.

1. Published at SOUPS 2021 [101]: "Never ever or no matter what: Investigating Adoption Intentions and Misconceptions about the Corona-Warn-App in Germany."
2. Published with honourable mention at CHI'23 [100]: "Less About Privacy: Revisiting a Survey about the German COVID-19 Contact Tracing App."
3. Published in Human Factors in Privacy Research [77]: "Privacy Research on the Pulse of Time: COVID-19 Contact-Tracing Apps."
4. Under Review for TOCHI: "I have not understood but agree. Studying informed consent in the context of the German COVID-19 contact tracing app."
5. Under Review for SOUPS 2024: "Can Johnny be a whistleblower? A qualitative user study of a social authentication Signal extension in an adversarial scenario."

The rest of the dissertation is structured as follows.

Chapter 2 This chapter presents three survey studies about the CWA and the necessary technical and historical background.

> **Section 2.1**: This section describes the functionality of digital contact tracing, more specifically the CWA, its context, and related work relevant to the studies.
>
> **Section 2.2**: The first study captured the intention to install the app, perceptions, and assumptions of the functionality of German participants before the release of the CWA.
>
> **Section 2.3**: The second study compares those results to the reported behavior of a second sample just after the release of the CWA.
>
> **Section 2.4**: The third study, motivated by many found misconceptions, focused on those in detail and investigated whether those misconceptions were found not only with non-users but also with users.

Chapter 3 This chapter presents two lab studies about a new protocol to exchange public key material, so called *authentication ceremonies*. In a whistleblower scenario participants should detect PITM attacks and react accordingly.

Chapter 4 Finally, I have drawn a conclusion to the results in light of what I learned from the studies, how closely perception and reality matched, and what we can learn from that.

Chapter 2

Case Study: Corona-Warn-App

FIGURE 2.1: Logo of the Corona-Warn-App. [164]

This chapter is about the first software I investigated: the Corona-Warn-App (CWA). The Corona-Warn-App (CWA) is a smartphone app utilized in Germany during the COVID-19 pandemic to do contract tracing digitally. I conducted three survey studies with a total of 1933 participants. In the first study, presented in Section 2.2, I researched the intention to install the app and what features were known to participants before the release of the app. After the release, I conducted the same study with slight adaptations to measure the intention behavior gap and to learn how the knowledge and reasoning developed over time. The study is presented in Section 2.3. Both studies showed that participants had a very vague idea of how the app does work. Similar results were made in other studies. Therefore, I conducted a survey that investigated the knowledge of users and non-users of the CWA in more detail. I was interested in whether the knowledge differed between these two groups. The study is described in Section 2.4.

2.1 Related Work

Before describing the three studies, I give a short introduction to the historical context of the CWA and explain how the app worked. After that, I give an

FIGURE 2.2: The Figure shows a comic that visualizes how the Corona-Warn-App works [33]. Without additional logging, no one knows the identity of an infected contact.

overview of related work on contact tracing apps that are relevant to all three studies that I conducted. Please note that most publications that are referenced were published after the studies were conducted. The first two studies were conducted in 2020, and therefore, there was little specific related work to build upon. The related work specific to each conducted and presented study, e.g., historical context or a relevant theoretical framework, can be found within the corresponding subsections.

Disclaimer: The contents of this section are based on previously published literature [101, 100, 77]. Details about my contribution to [101, 100] can be read in the corresponding section about the publications (Section 2.2 and Section 2.3). With [77] my co-author Eva Gerlitz and I contributed a chapter about contact tracing to the book "Human Factors in Privacy Research". We shared the load of the literature review and discussed our findings.

2.1.1 Contact Tracing

In 2020, COVID-19 hit the world, and with it came the desire for a well-functioning and fast-working possibility to trace contacts of those people who tested positive for the virus, a method called *contact tracing*. Contact tracing is following the Cambridge Dictionary, "the process of finding any other people that an infected person has met or had close contact with, usually in order to control the spread of an infectious disease" [40]. Similar definitions are used

elsewhere, e.g., by the World Health Organization (WHO) [55] and the European Centre for Disease Prevention and Control (ECDC) [41].

Early on, digital contact tracing was seen as a tool to interrupt chains of infection. This led to a discussion about apps to automatically trace and store with whom a user had been in contact with and, as a result, would warn those who might have become infected. Digital contact tracing was even advertised as a "key" in fighting the pandemic [57]. It has several advantages compared to a manual approach done by health workers, e.g., it enables warning more people who otherwise could not have been notified due to incomplete memory or knowledge about contacts of an infected person. Digital contact tracing also supports the authorities with the work load that comes with notifying contacts of positive tested persons: Instead of calling each person one-by-one, the information can be transferred immediately to all persons at once.

Most of the digital contact tracing approaches in 2020 were realized through smartphone apps. The idea of using apps that help fight a disease was not new in 2020. In Africa, e.g., an app supported contact tracing personnel in faster submitting the information to help combat Ebola in 2019 [183].

One of the first COVID-19 focusing apps was launched in February 2020 by the Chinese government. It was specifically designed to warn its users about contact with someone who is infected with the virus [35]. Many other governments followed, and a lot of those contact tracing apps (CTA) based their tracing on Bluetooth or the users' location. In March 2021, the MIT Technology Review listed 49 contact tracing apps in 48 countries from around the world [2] and an overview from Google lists 60 apps that make use of their provided framework [167].

Depending on how automated tracing is implemented, it is necessary to capture and store sensitive information about the user, such as where the user has been, who they were in contact with, and their health status. All of this entails the potential of mission creep and surveillance if going beyond the primary purpose of the tracing technology. Based on the possibility of misuse, a lot of public discussions in 2020 revolved around the architecture of such tracing apps. Many experts and organizations worldwide made a strong statement for apps that technically prevent such abuse [42].

Researchers from the University of Oxford estimated what percentage of the population would need to install a contact tracing app for it to be effective, depending on further measures that were taken throughout the country. Their results indicate that adoption of 60% could stop the pandemic, but already smaller installation numbers would reduce the number of infections and deaths [107]. In public discussions, this number of 60% was often misreported to be the threshold that needs to be achieved in order to fight COVID-19 [150].

Taken together, the requirements of being privacy-preserving and the need to reach a large part of the population were able to influence political decisions, e.g., in Germany [47], where the government switched to a more privacy-preserving app after another one had already been planned. Because all the

presented studies in this dissertation evolved around the CWA we detail the situation in Germany later in Section 2.1.1.

Tracing Technologies This section gives a brief overview of technical possibilities to automatically warn people who had been in contact with someone who later tested positive for COVID-19. Different versions of contact tracing apps were proposed, discussed, and rolled out worldwide. The task of apps in this context ranged from simply informing users about their contact and asking them to start a voluntary quarantine (e.g., in Germany [157]) to functioning as access control (e.g., in China [147]).

Obviously, it is (currently) not feasible to technically directly trace whether a person met another person; therefore, many solutions use the personal smartphone as a proxy. The apps captured whether a device was in proximity to another device; therefore, it the technique is also called proximity tracing. For simplicity, we assume in the following that people always carry their smartphones with them, and we will use the ideas of "Who met whom" and "Which device encounters which device" interchangeably.

The following two sections detail the steps of such a digital contact tracing: The tracing itself and the details of when and how a user is informed about meeting someone who tested positive. Our goal is to give enough detail about the essential technology so that the reader can have a general overview and follow the rest of the dissertation.

Proximity Tracing For a contact tracing app to work, first and foremost, it must be logged who was in contact with whom. There are different approaches to accomplish this and different ways to categorize them: Huan et al. [110] for example, used a categorization where approaches are separated based on the data collection method: *cell phone base station data*, *location history*, and *Bluetooth proximity data*. Another possible taxonomy could be built based upon the interaction and setup needed (e.g., device to device communication directly via Bluetooth), indirect via participation tracking (e.g., at an event through QR codes [67]), or the not-so-common usage of already existing data (e.g., cell phone base station data).

To understand a lot of the research focusing on contact tracing, one has to look at the storage location of the logged contact data and the usage of Bluetooth Low Energy (LE). The usage of other technologies, such as WiFi, to track devices within reach of an access point are thinkable but where not utilized in the pandemic. Similar techniques are used in other areas, such as occupancy estimation [113] or trying to detect burglars [190]. Instead of providing a central body, such as a health organization, with information about the number of people's contacts and thus estimating the potential spread of the disease, many contact tracing apps focused on alerting individuals and worked as follows: devices broadcast IDs via Bluetooth LE. The received IDs are stored together with

the sent ones, and some information is added/derived, such as a distance and time metric. Those stored received IDs are later matched with a list of IDs representing infected persons. If a device keeps the gathered IDs stored locally and compares them locally to a public list of IDs representing infected persons, the approach is called *decentralized*. On the other hand, *centralized* means that the devices of infected persons upload at least the seen and gathered IDs to a central entity/server.

Both approaches have their disadvantages, but the threat model differs. In the centralized approach, parties having access to the service (e.g., the hoster or the government) could gain access to the data [170]. In this case, the party having access to the data could, for example, learn about the users' social graph. Compared to this, in the decentralized approach, an attacker needs to be in close vicinity to gain knowledge, as explained by Baumgärtner et al. [16].

Independent of how the approaches are categorized, tracing was discussed in many different ways, and for further research in this area, we suggest further literature and projects (e.g., [61, 158, 12, 178, 16]).

Risk Calculation and Informing those at Risk For efficient contact tracing, it is not only necessary to trace contacts, but also to inform those who had been in close contact with infected people (and possibly also give advice or instructions on how they should behave). This can be divided into the following three problem spaces:

Medical basis for risk calculation: The fundamental question is who should be informed and under what circumstances. For this, requirements from epidemiologists and virologists need to be implemented, concerning, for example, the distance and time after which an infection becomes more likely.

Technical implementation of risk calculation: There are different possibilities for where the actual risk calculation can occur. Research and politics in the EU favored mainly the previously outlined decentralized approach. In this approach, the assessment of whether the user is at risk is calculated on the phones directly. In the centralized approach, this calculation happens on a central server. Independent of the approach is the fact, that the risk calculation can only be an estimation of what actually happened. False positives and true negatives have to be balanced. On either side, it can result in a negative effect on the adoption and effectiveness of the app.

How to inform those at risk: In the decentralized approach, no central entity knows who is infected and therefore cannot inform them. Each device itself is "responsible" to inform its user. In a centralized setting, the server knows who is at risk. Therefore, even out-of-band contact, e.g., via phone, is possible depending on what data is available.

Contact Tracing in Germany

In Germany, mainly two approaches to collect and process data for contact tracing were discussed for an official app. In the centralized version called "Pan-European Privacy-Preserving Proximity Tracing" (PEPP-PT) [159] all collected encounters, namely contact-ID and timestamp of encounters with other app users would be uploaded and stored on a central server. In the decentralized version "Decentralised Privacy-Preserving Proximity Tracing" (DP-3T) [61], all encounters remain on the users' smartphone. If a user tests positive for COVID-19, they can upload all their cryptographic keys (from which the IDs can be derived) to a server. Once a day, a list with keys of people who reported their positive COVID-19 tests is downloaded to all users' smartphones and compared to locally stored encounters within the last 14 days. At the beginning of the discussion, the German government wanted to follow the centralized approach [161]. After two open letters in April 2020 suggesting the usage of DP-3T [42, 154], the German government changed course and pivoted to the decentralized approach on April 26 [47]. Two days later, a press release was published that contained (technical) information about the app, such as that it would work with Bluetooth [165].

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 centralized approach that was then discarded [161]. The CWA was finally introduced in June 2020 and followed a decentralized approach for contact tracing based on the Exposure Notification System of Android and iOS [49, 27]. It used Bluetooth to collect encounters with other devices [50] and no GPS data was gathered or used.[1] The development and operation costs for 2020 amounted to €52.8 million [31] and were estimated to add up to more than €200 million by the time the app was retired on May 31, 2023 [79]. The government promoted the app through an advertisement and education campaign [96, 28]. The app received positive feedback for its architecture [229] and criticism concerning the project's political handling [231].

After its release, at least for a while, 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., [197, 195, 230, 231]) and private media (e.g., [18, 184]).

2.1.2 User acceptance of tracing-apps

Since the idea to use apps that would support the contact tracing work of the health departments to contain COVID-19 became popular among governments worldwide, researchers aimed at understanding user preferences to allow for

[1] For more information please visit the official website [49]. The source code of the app is available on GitHub [89].

broad adoption. Studies were conducted in Australia [202], Europe [182] (including Belgium [218], France [9, 94], Germany [108, 124, 24, 128, 9, 208, 205], Italy [9], Ireland [151], Switzerland [227] and the UK [223, 222, 109, 15, 9]) and the USA [103, 124, 131, 233, 9, 99, 208, 182, 132, 74, 118, 220, 170]. As Utz et al. [208] and Kostka et al. [124] found similarities for Europe and America, and we are interested in studies we can relate to the situation in Germany, we focus on work conducted with those populations.

Many early conducted studies were choice-based conjoint experiments, in which participants were asked to select which app of several they would prefer or were given different app configurations for which they had to decide if they would install such an app [208, 24, 233, 222]. Some studies asked to imagine a corona tracing app has already been released [9, 109, 124, 103, 131, 218] We are aware of only a few early studies that looked at the user acceptance and influencing factors on the acceptance for the app that was already launched in the surveyed country [202, 227, 143].

Investigated Factors

The studies explored factors that could influence participants' intention to install and use the corona tracing app. Several authors investigated how personal characteristics, such as demographics or one's experience with the pandemic, impacted the acceptance of corona tracing apps [108, 103, 124, 131, 227, 15, 233, 24, 9, 99, 208, 94]. Amongst others, people who were male [108, 131, 208], had higher trust in the respondent's government [227, 24, 9, 208, 94], health authorities [227] and others in general [108], had higher income [131, 227] or lived in urban areas [124, 131] were more likely to install a tracing app. While some authors noted that younger participants were more inclined to use a tracing app [108, 131, 99], others found the opposite [103, 124]. Looking at pandemic-related factors, health concerns during the pandemic, and personal experience with COVID-19 increased the willingness to install a tracing app [124, 24, 99, 208, 94]. Additionally, better adherence to COVID-19 regulations was a positive influence [227]. Fear and anxiety concerning changes in government rules [15] impacted participants negatively.

Apart from factors that might influence the acceptance of contact tracing apps in general, many studies were conducted to find which app design choices would be considered positively or negatively by participants. The studies covered different attributes (e.g., what data will be collected) [131, 233, 24, 118, 132], the apps purpose [208] or what institution will develop, host, distribute or own the app [222, 109, 24, 99, 182, 220, 170]. Li et al. [132] found a preference for the centralized model, while Zhang et al. [233] had more participants who were willing to use an app based on the decentralized approach. Horvath et al. [109] found a centralized national health system to be favored. Participants rated health agencies more trustworthy than their government as a whole concerning corona tracing apps [182, 109]. Still, Simko et al. [182] found no entity that

everyone trusted. Anonymous data collection impacted participants positively in their decision to use an app [24] and it was perceived negatively if the collected data can uniquely identify individuals [208]. Independent of app design choices, studies often found a subset of participants who did not like any of the proposed apps [132, 208, 118].

Aside from app properties, researchers looked into effects an app could have, and the influence this has on adoption [222, 131, 24] such as malfunctions of the app [208, 118] or the perceived effectiveness in fighting against COVID-19 [124, 128, 218, 131]. They found that participants' perception of the (public) health benefits an app would offer and other people's willingness to use it explained the usage intention better than app design choices and personal characteristics [131]. Performance expectancy and the benefit were also among the most critical predictors in other studies [218, 124, 128]. Malfunction in contact tracing was found to be of negative influence [208] and participants valued false negatives worse than false positives [118]. The willingness to use contact tracing apps increased if its usage is linked to priority testing [222, 24]

Further, numerous studies identified the primary reason why users would or would not install tracing apps [108, 223, 227, 15, 9, 151, 208, 202]. In their studies, privacy concerns [202, 108, 227, 15, 9, 223, 208], technical concerns or lack of technical equipment [202, 108, 227], distrust in the government [202] or the fear of surveillance at the end of the pandemic [9, 151] and doubts about the effectiveness or benefit [108, 227] were brought up as negative influences. The following topics were mentioned as reasons for using a tracing app: willingness to protect family and friends [9, 151], a sense of responsibility for the community [9, 223, 151] and the hope that the app may stop the pandemic [9].

2.1.3 Knowledge about corona tracing apps

If someone wants to install an app based on their properties one has to know them. The subsequent listed studies are an excerpt about what participants knew about corona contact tracing apps in general or a specific one.

Knowledge Worldwide Simko et al. [182] conducted surveys for seven months in the US and Europe, focusing on contact tracing and privacy and asking for potential app properties. Within the participants' answers, they identified several false mental models, e.g., that proximity tracing is less secure than location tracking due to constant communication between devices. Zhang et al. [233] surveyed 2000 participants in the USA to measure the support for nine different COVID-19 surveillance measures, including tracing apps. While analyzing, they noticed participants had many misunderstandings about the described app, although the description was still visible when they answered the questions. For example, a third believed they would receive the names of infected people they had been in contact with. The number of incorrect answers could not predict the participants' usage intention. Williams et al. [223] conducted focus groups in the

UK to explore public attitudes to the proposed contact tracing app. The authors found the most common misconception was that the app would make it possible to precisely identify COVID-19 cases in their vicinity and amongst their contacts. In one study that took place outside Europe and America, Thomas et al. [202] surveyed 1500 Australians after the national tracing app was released and examined participants' knowledge about it. Around 70% knew the app would make it easier and faster to inform people exposed to COVID-19 and warn users who would not have been warned otherwise. However, 50% did not reject the assumption that their personal information would be used after the pandemic, and 57.4% believed the app would warn if infected people were near them.

Knowledge in Germany Four studies investigated knowledge that German participants had about the CWA: Kulyk et al. [127] who surveyed 135 participants between December 2020 and February 2021, Munzert et al. [148], who surveyed and/or traced the app behavior of over 2500 participants. Some participants were also educated about the app, Kozyreva et al. [126], who sampled 4357 participants in four waves (two of which were conducted after the app's release), and Meier et al. [143], who presented 952 participants ten statements about the CWA.

However, connecting the various studies to get a complete picture of participants' understanding of the app proves to be challenging: first, the studies were conducted at different times during the pandemic. Kulyk et al. [127] reported that 63% of the participants knew that the app uses Bluetooth. Kozyreva et al. [126] asked for the participants' awareness of the technology used twice and found that between the end of August and the beginning of November 2020, around 10% fewer participants were aware the app used Bluetooth (August: 76% of the app users, 35% of non-users; November: 65% of the app users, 26% of non-users).

Second, the questions posed in the different studies do not always align. Munzert et al. [148] and Kulyk et al. [127] both inquired about the location where the app's data was stored. Munzert et al. asked whether "[d]ata collected by the app [were] stored centrally at the RKI", with 30% of the participants from the control group correctly marking this statement as incorrect. On the other hand, Kulyk et al. [127] presented participants with three statements regarding data storage: "[l]ocally on my phone", "[c]entrally with the government", and "[c]entrally in a company". Over half of their participants believed that data was stored locally on their phones, almost 30% thought data was stored with the government, and nearly 40% believed the app's data was stored centrally in a company. It is evident that both studies did not differentiate between encounter data and infection status, which impacts factors such as data storage location.

Meier et al. [143] did not present the descriptive statistical results of the participants' knowledge in their study. Similarly, Kowalewski et al. [125] included

knowledge-related questions in their survey of a German sample but did not report the results.

For these reasons, within our surveys, especially the third presented in Section 2.4, we asked for different aspects of the app separately and in detail to get a holistic and exact overview of the participants' knowledge.

Misconceptions and Uncertainty Numerous studies have highlighted misconceptions and misunderstandings regarding CTAs in several countries [202, 223, 182, 127]. For instance, some individuals believed that these apps could reveal current hotspots or identify infected people in their vicinity [202, 223]. Participants also misunderstood the consequences of Bluetooth and with some believing it was insecure [182] or could be used to track their location [17].

In the study by Kulyk et al. [127], over 40% of the German participants thought the government, health care providers, and developers of the app had access to the data collected by the app. That would not be a misconception if not additionally 72% believed the app would collect metadata, including geolocation information.

As the studies were conducted in different countries and focused on different apps, it is challenging to generalize these misconceptions to other countries and apps. Still, the literature provides evidence that there are many widespread misunderstandings about how digital contact tracing works and what the associated risks are. The papers published during the course of my dissertation were amongst the first to examine German participants' understanding of digital contact tracing and the influence of this on their intentions, behavior and perceptions.

2.2 Never ever or no matter what: Investigating Adoption Intentions and Misconceptions about the Corona-Warn-App in Germany

Disclaimer: The contents of this chapter are based on the published paper "Never ever or no matter what: Investigating Adoption Intentions and Misconceptions about the Corona-Warn-App in Germany" presented at the seventeenth Symposium On Usable Privacy and Security (SOUPS) in 2021 [101], together with my co-authors Eva Gerlitz, Christian Tiefenau, Matthew Smith, Dominik Wermke, Sascha Fahl and Yasemin Acar. As this work was conducted with my co-authors as a team, this chapter will use the academic "we" to mirror this fact. The idea and initial concept for this publication came from Matthew Smith, Eva Gerlitz, and me. The survey was designed in collaboration with all co-authors and the persons mentioned in the acknowledgments of the publication. Christian Tiefenau, Eva Gerlitz, and I analyzed the qualitative and quantitative data. Dominik Wermke provided the knowledge and draft for the regression model. Christian Tiefenau, Eva Gerlitz, and I created the key observations and, before compiling the paper for publication, jointly discussed the study's implications with Matthew Smith, Sascha Fahl, and Yasemin Acar.

A major argument used for the decentralized approach (see Section 2.1.1) was that the general population would only be willing to adopt the app in sufficient numbers if privacy was preserved ("It is crucial that citizens trust the applications") [42]. The German government had previously committed to an app based on the centralized approach, which they abandoned during development due to the public debate, starting a new development project based on the decentralized approach at the end of April. The media extensively discussed this decision, and the government, via direct appeals and public media, encouraged people to install the app. In this context, we were interested in finding out how much the general public understood about the newly announced app. We were also interested in the general public's attitudes towards potential properties, particularly those about the advantages and disadvantages of the centralized and decentralized approaches. To gain insights into these issues, we conducted an online survey study from May 30 to June 11, 2020, with a quota sample of 744 participants from Germany.

In the following subsections, we make the following contributions:

- We conducted a study to assess participants' knowledge of and beliefs about the planned CWA after the app features were published and broadly discussed in the media. This is in contrast to other studies in Germany that focused on hypothetical apps.
- We assess *how accurately* participants could identify the properties of the planned German contact tracing app.

- The German public discourse was dominated by the discussion of a centralized versus decentralized application. We offer insights into the level of relevance of the app's capabilities linked to the centralized approach.
- We compare our work to contemporary work that assessed willingness to install various hypothetical tracing apps in Germany[208].

2.2.1 Methodology

The following subsections describe instrument development and the conducted survey, our recruitment, and the data analysis process.

Survey Development

We followed the public discussion of the CWA. We were interested in the information that potential users have, mainly as discussions focused on whether enough people would install it and why (not). Much of this discussion in Germany revolved around the topic "centralized versus decentralized" and the claim that this would heavily influence the willingness to install. Not only connected to this we were also interested in the broader topic of acceptance and beliefs. We discussed factors and potential influences with other researchers and iterated multiple times over the survey.

Pre-Testing Before handing out the survey, we conducted several test rounds with colleagues who were not involved in the survey creation to identify comprehension problems. Following that, we asked 19 computer science students to fill the survey and provide additional feedback about unclear sections and inconsistencies. After this, we additionally sampled 50 participants on Clickworker [36]. Finally, we asked five participants without a technical background to fill the survey while thinking aloud. Before starting the final study, Qualtrics [168] additionally sampled 50 people. This pilot study helped get an overview of the duration, evaluate the randomization and spot flaws in the survey logic.

Survey Content

To inform the survey structure and questions, we looked at the different available approaches to develop a contact tracing app and followed the media discussion. The final survey consisted of the following described four parts and can be seen in Appendix A.1.

Media Sources and Knowledge In the first part, we asked whether the participants had already heard of the planned app and asked for their knowledge

sources (e.g., public broadcasters, family members, social media, or official government websites) (Q7). After this, we asked questions that assess their knowledge of the properties of the app in general (Q8). We also asked such questions for two scenarios: what happens if other users are infected (Q9) or if the users themselves are infected (Q10). In these three question blocks, we included 23 statements that were either correct (8 statements) or incorrect concerning the soon-to-be-released app (15 statements). As incorrect statements, we used properties of another 'corona app' released in Germany [43][2] or were discussed in media at the time of the survey. For example, we included the misconception that the app will share all phone numbers saved on the user's phone or share a movement profile with the government. Three statements were neither correct nor incorrect for the released app. Details of all these statements can be found in Table A.2.

Disposition to use In the second part of the survey, we showed the participants a minimal description of the app, including the information that its primary purpose will be to warn users who have been close to infected persons and use Bluetooth to detect other app-users. Following that, the participants were asked whether they are planning to use the app, using a question with five possible answers ranging from "1 - Definitely will use it" to "5 - Definitely will not use it" (Q12). We also asked to report their primary reason for their choice in a text field (Q13).

Potential Properties The third part presented 23 hypothetical statements, from now on called *potential properties*, about the app (Q14). The participants were asked how these statements would affect their willingness to use the app if the app would work this way (5 answer options, from "1 - Definitely would use it" to "5 - Definitely would not use it"). In this section, we added an attention check question. Six of those properties can be attributed to a centralized approach, while one would only be valid for the CWA app that is based on the decentralized approach. Additionally, 12 properties were correct for the to-be-released app, while 11 were incorrect. Details of all the presented statements can be seen in Table A.3.

Demographics In the end, we asked for demographic data and how COVID-19 impacted their lives (Q16-29).

[2]The app can be used to share fitness data with the RKI.

Recruitment

We used Qualtrics[168] to recruit a representative German sample according to age, education, household income, and federal state/region. Qualtrics provided representative numbers for age, education, and region, numbers for income were taken from the Federal Statistical Office of Germany from 2017 [63]. Due to the nature of online surveys, older participants were underrepresented, and we could not entirely fulfill our quotas for a representative sample. The final distribution after sanitizing the data together with our targeted quotas can be seen in Table 2.1. The study was conducted from May 30 to June 11; thus, shortly before the app was launched on June 16, 2020. To take part in the study, it was required that the participants owned a smartphone since that is a precondition to use the app. 1025 participants took part in the study for which we paid Qualtrics € 4000.

Data quality

During the study, Qualtrics excluded participants that 1) took less than half the median of the time the participants needed in the final pilot study (243 seconds) for completing the survey, [3] or 2) failed the attention check question in the potential properties question block.

To ensure our participants were paying attention, we included a straightforward attention check (Q14) and one comprehension check question (Q11). The comprehension check question gave a short explanation of how the app will work (specifically mentioning using Bluetooth for contact tracing). It then asked what technology the app will utilize for contact tracing. We excluded participants from our analysis who did not choose "Bluetooth".

When we designed this question, it seemed quite straightforward. To our surprise 262 participants failed this question. We then discussed whether we had overlooked genuine reasons why this question might be answered incorrectly. Potentially, participants who read our description text did not believe it and answered true to their previous or internal beliefs. It is also possible that our description was too complex for some to understand and thus could mean that they misunderstood other questions.

We also discussed the possibility of excluding participants due to inconsistent or odd answers, e.g., a participant stating that they are a civil servant but also stating that they lost their job[4] or stating that the app used Bluetooth in one question and stating otherwise in another. However, after an in-depth discussion, we decided against this. We looked at the free text answers of participants who had such inconsistencies, but we found them generally to be as plausible as those who did not and did not find any other warning markers.

[3] This is a standard procedure at Qualtrics; we do not know how many participants were excluded.

[4] In Germany this combination is incredibly rare.

Analysis

We analyzed the data in two different ways. Most of the results concern a quantitative analysis of the answers. One free text answer was analyzed qualitatively. Percentages are reported rounded.

Quantitative For our quantitative evaluation, besides reporting, we performed an ordered logit regression with model selection, an ordered logit regression model containing all potential properties, and hypothesis testing. For the app usage intention, we decided to combine participants who answered "I don't know" and those who answered "I am undecided".

In the *Media Sources and Knowledge*-section (Q8-10) of the survey, we asked participants whether they thought the presented statements were correct for the CWA. False statements required no click from the participant to give the correct answer. This may influence the measured correctness of their beliefs, besides the point that some statements may be easier or harder to know. We, therefore, only report true statements that were known as (positive) knowledge and false statements that were clicked as false beliefs.

Coding process Participants were asked to indicate their primary reason for wanting to use or not use the CWA (Q13). One researcher looked at the answers and coded them according to the participant's misconceptions. All presented quotes were discussed and agreed upon by two researchers. All quotes were originally in German and translated into English by the authors.

Regressions For our exploratory regression model, we conduct a model selection approach by computing a set of candidate models based on different factor combinations, and selecting the final model based on a combination of the best Akaike Information Criterion (AIC) [32] and Bayesian Information Criterion (BIC) [3]. Possible factor categories and corresponding baselines are reported in Table A.1.

Our final ordered logit regression (cf. Table 2.2) reports change as log odds to highlight trends: a negative value directly correlates to a negative effect and vice versa for positive values. In addition, we report a 95% confidence interval (C.I.) and a p-value. For convenience, we highlight factors below an arbitrary significance cut-off of 0.05 with an asterisk ($*$).

In addition, to investigate potential effects of different app features, we conducted an ordered logit regression (cf. Table 2.3) with all app features as factors.

Ethics

Our study was reviewed and approved by our institution's Research Ethics Board. We also adhered to the German data protection laws and the GDPR in the EU. For all answers, we provided an option for participants not wanting

to give any details (i.e., "I don't want to state" or "I don't know"). Participants could drop out at any time. Participants had to consent to take part.

Limitations

We aimed for a representative sample of the German population. Unfortunately, some groups are over- while others are underrepresented. Our sample lacks people of older age, people with lower education, and those with high income. Qualtrics, who acquired the sample for us, stated that this is very common in online surveys. As with every survey study, we have to take into consideration that the data is self-reported. In this study, we additionally asked participants about their future behavior, which is even more prone to uncertainty. Many possible properties of the app have consequences that are not easy to estimate. We cannot assume that participants understood and thought of the consequences, especially considering many participants did not understand how the app worked in detail.

2.2.2 Results

In this section and the associated subsections, we present the results of the survey. We describe our participants, the accuracy of their knowledge about the CWA, and what sources they consulted. Following that, we describe the participants' intention to use the app and how demographic factors and beliefs about the app explain this decision. Last, we describe how different potential properties, such as additional features, influence the willingness to install the app.

To avoid confusing and overly complicated figures, we assigned short identifiers to each question, which can be seen in Table A.2 and Table A.3.

Demographics

Table 2.1 presents the demographics of the final 744 participants and Table A.4 gives an overview of how COVID-19 impacted them.

Since we conducted the study at an early stage of the pandemic, few participants had fallen ill with COVID-19 themselves or had somebody close to them fallen sick. 31.1% count themselves as being a member of the high-risk group. This may seem high but matches estimations in Germany [172]. Around half reported that the pandemic did not influence their work situation (52.7%). 24.5% work from home, and 13.6% reported working in short-time. 74.9% said they did not have specialized tech skills. According to the "Sonntagsfrage" [221],[5] our sample includes 20.7% fewer participants who would have voted

[5]Regular opinion research in Germany, asking, "Which party would you vote for if federal elections were held this Sunday?"

Gender	**Female**	55.9	**Male**	43.3	**Other**	0.8		
Age	**18-24**	24.2 (9.2)	**25-34**	14.3 (15.3)	**35-49**	23.9 (23.9)	**50-64**	26.8 (26.4)
	65+	10.9 (25.1)						
Education	**ISCED 0-2**	5.9 (16.5)	**ISCED 3-4**	48.9 (58.1)	**ISCED 5-8**	40.5 (25.4)	**Not disclosed**	2.2
Household	**<= 1300€**	18.3 (16)	**1300-1700€**	13.4 (8)	**1700-2600€**	20.8 (20)	**2600-3600€**	16.7 (18)
Income	**3600-5000€**	14.0 (17)	**>5000€**	6.2 (20)	**Not disclosed**	10.6		
Work Status	**School student**	4.7	**Univ./col. student**	9.8	**Employee**	48.9	**Civil servant**	2.0
	Self-employed	4.6	**Freelancer**	2.2	**Unemployed**	7.5	**Retiree**	16.9
	Not disclosed	3.4						
IT-Knowledge	**Yes**	20.9	**No**	74.9	**Not disclosed**	4.2		
Smartphone OS	**Android**	71.5	**iOS**	26.1	**Other**	2.4		
Political	**The Greens**	21.6	**CDU/CSU**	19.4	**SPD**	11.7	**FDP**	6.7
Affiliation	**AfD**	6.1	**The Left**	10.1	**Others**	24.5		
Federal state	**BW**	12.9 (13.1)	**BY**	12.1 (15.6)	**BE**	7.0 (4.3)	**BB**	2.4 (3.1)
	HB	1.5 (0.8)	**HH**	3.6 (2.2)	**HE**	6.9 (7.5)	**MV**	2.4 (2.0)
	NI	6.7 (9.6)	**NW**	22.9 (21.6)	**RP**	4.6 (4.9)	**SL**	1.5 (1.2)
	SN	5.0 (5.0)	**ST**	4.7 (2.8)	**SH**	3.5 (3.5)	**TH**	2.4 (2.7)

TABLE 2.1: Participants' demographics (N= 744), in percentages. Numbers in brackets = the targeted distribution [168, 63].

for the CDU/CSU[6] at the time the survey was conducted, but 6.6% more participants who would vote for The Greens. All other parties are close to the percentages of the "Sonntagsfrage". We hypothesized the party preference might be an indicator of the attitude towards the app as at least one party publicly criticized the app [191].

Knowledge

We asked participants to select what they believe are correct statements about the app (Q8-10). As the app was not released when the survey was conducted, answers were not based on experience with the app. However, a press release had been publicized that gave information about the app [165], such as that it would use Bluetooth-Low-Energy, that its primary purpose would be to warn users who had been in close contact with infected people, and that users would not learn who of their contacts reported an infection. At the same time, much misinformation about the app, its purpose, and technical details were spread as well[29].

This section describes the sources participants used and presents participants' beliefs about the to-be-released CWA.

Sources We asked the participants whether and where they heard about the planned corona app (Q7). Figure 2.3 shows the frequency of how often the participants reported a source. Please note that as participants could report more than one source, the percentages do not add up to 100%. Few but a non-negligible amount of participants (11.7%) reported to never have heard of the app. This leaves 657 participants who were at least somehow aware of the app.

More than half of the participants (54.7%) reported that they received information about the app from public broadcasters. The second most common

[6]The Christian Democratic Union of Germany / Christian Social Union in Bavaria

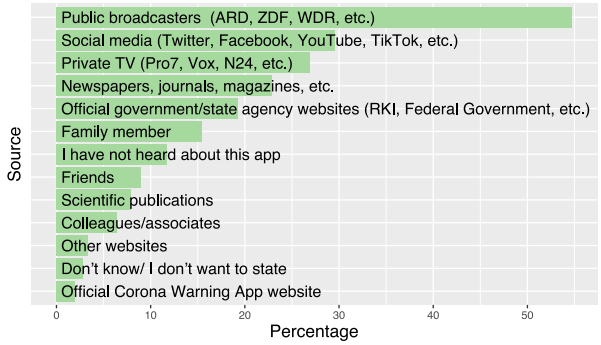


FIGURE 2.3: Frequency of reported information sources (n=744).

marked source was social media (29.6%), such as Twitter or Facebook.[7] Scientific publications were used by 7.9% to get information about the CWA.

Correctness of assumptions The following paragraph gives an overview of the participants' assumptions about the CWA (Q8-10). It should be noted that we only included participants who previously reported that they already heard about the app (n=657).

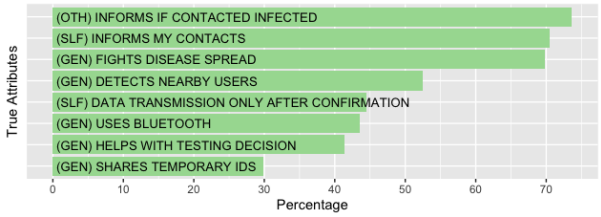


FIGURE 2.4: Attributes that are correct for the current app and the percentage of participants who checked the corresponding box. OTH: other is infected, SLF: self infected, GEN: general attribute.

Figure 2.4 depicts the correct statements for the app that was shortly released after the survey was conducted and shows how many participants marked those to be true. Figure 2.5 shows all statements that are false for the released app. We classified participants who marked any of the false statements as correct as having "False Beliefs".

59.5% of the participants knew about the app's basic functionality, i.e., that it would warn its users when they had been in contact with another user who later tested positive (`(OTH) INFORMS IF CONTACTED INFECTED` and `(SLF) INFORMS MY CONTACTS`). Around half of the participants knew about the detailed flow that a lab has to confirm the infection before it can be registered in the app (`(SLF)`

[7] Following a statistic from Statista, 65% of the citizens use social media in Germany in general [11].

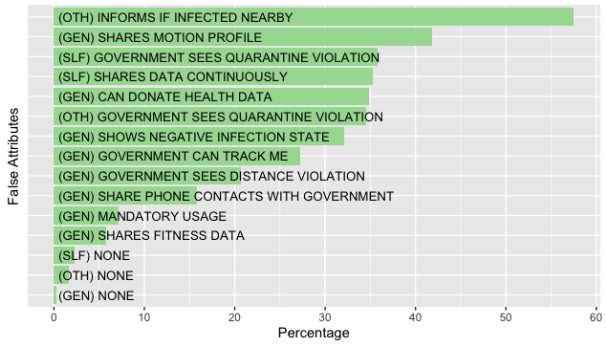


FIGURE 2.5: Attributes that are wrong for the current app and the percentage of participants that checked the corresponding box.

`DATA TRANSMISSION ONLY AFTER CONFIRMATION`) to prevent misuse of the app and many false warnings.

However, the app's technical basis was less known: Only 29.8% of the participants who reported to have heard about the app knew that the app would share temporary IDs and timestamps, and 43.5% were aware the app would use Bluetooth. At the same time, 54.6% of the participants thought that the app would use location services, and 24.7% believed the app would use Bluetooth and location services in combination. Although Bluetooth is not a technique developed for position finding, it is, next to GPS, listed as a "location service" in some circumstances [20]. We assume that only participants who marked Bluetooth and location service could have been aware of this detail. 30.0% did not think the app would use Bluetooth but checked location services.

A common misconception (57.5%) was that the app would warn users if an infected person is in their vicinity.

9.89 % of the participants knew all the information that was included in the official press release about the app (`(GEN) SHARES TEMPORARY IDS`, `(GEN) DETECTS NEARBY USERS`, `(GEN) USES BLUETOOTH`, `(GEN) FIGHTS DISEASE SPREAD`, `(OTH) INFORMS IF CONTACTED INFECTED`, `(SLF) INFORMS MY CONTACTS` [165]).

On average, the participants correctly recognized around half of the eight aspects that are true for the app ($median = 4, mean = 4.26, std = 2.05$), but none was known to everyone. Only five participants marked all correct attributes as such and did not believe any incorrect statement.

We asked for the classification of two statements (`(GEN) RESTRICTS BASIC RIGHTS`, `(GEN) THREATS PRIVACY`) that cannot be classified as correct or incorrect but are based on personal sentiments. We saw that participants were worried about their privacy in combination with the app (27.4%) and their basic rights (20.1%). 14.9% stated both in combination.

Misconceptions and lack of information After asking participants how likely they will use the app (Q12), we asked for the primary reason for their installation intention (Q13) in free text form. As we saw many false beliefs, we coded the

answers according to underlying misconceptions. We saw statements that were incorrect concerning the app's functionality and its data usage.

Some statements we observed were incorrect but might be correct with the further context of the answer. Participants who (probably) wanted to use the app, for example, stated: *"My safety"*, *"To protect myself"* or *"I want to stay healthy"*. Since the app cannot protect its users directly (users have already been exposed to infected people before they are warned) but only indirectly (the more people download the app, the more people might be influenced and will also download it, leading to better protection of all of its users), these answers indicate a misunderstanding of what the app can do for individual users.

Other answers were incorrect beyond doubt. One participant, for example, thought they would be able to see the number of current infections: *"To follow the spread of the pandemic"* (Probably will use the app).[8]

As already seen in Figure 2.5, participants believed the app would inform its users if infected people are close. This argument was used both as a positive as well as a negative reason to use the app. One participant probably wanted to use the app and argued: *"So I can see who is infected nearby to keep a larger distance to them and protect myself and fellow people."*. Another one did not want to use the app and wrote: *"The determination of the location is too inaccurate. It might happen that other people see me as infected, even though it is somebody else. I have concerns that this might lead to public hostilities or bullying."*

Participants also misunderstood what data will be used and shared: *"I don't want the government to know where I am in each and every second - especially as three other companies are involved as well"*[9] (Definitely will not use it) and *"I don't want the government to have all my numbers and names"* (Definitely will not use it).

Additional to the location misconception, we observed a participant who believed it would be necessary at all times to have access to the internet: *"I don't know how it works but if I need internet you can already forget about it, as I don't have mobile data."*. Anecdotally the participant was not able to correctly answer that the app will use Bluetooth.

Participants indicated that they are confused by the amount of (different) information: *"I don't have any trust. With all the news, I don't know what to believe anymore!!!"* (Probably not use the app). One participant, who failed the comprehension question and was undecided about the app, said: *"Everybody says the opposite of the others. Many say you lose your privacy."*

Following these answers and the data reported previously in this section, we conclude that many participants did not wholly understand the apps' functionality and thus assume a misconception in who will be protected by the app, what data it collects, and with whom the data will be shared.

[8] This is, in fact, possible since version 1.11 which was released at the end of January 2021 [216].

[9] It is not fully clear who the participants refers to. Telekom and SAP developed the app. Two research institutes advised. The RKI is publisher [51]

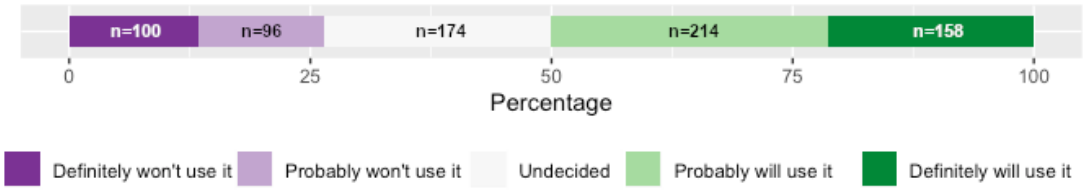


FIGURE 2.6: Reported intention to use the app.

Intention to use

Figure 2.6 shows the usage intention of all 744 participants. When looking at those participants who were very certain in what they will do, more participants indicated to definitely install the app (Def-Yes, 21.2 %) than to definitely not install it (Def-No, 13.4 %). Almost a third reported they will probably use the CWA (Prob-Yes, 28.8 %) compared to 12.9 % who reported to probably not use it (Prob-No). 23.4 % were still undecided (Undecided) about the installation. As of May 28, 2021 the reported download number of the CWA is 28 millions [122]. That estimates to around 46% of smartphone users in Germany [187]. This estimate does not take into account that that the same person could download the app onto multiple devices.

In the following, we report indications for reasons of the installation intention. For this, we selected an ordered logit regression with a model selection process via best AIC and BIC (c.f. Table 2.2). In the following paragraphs, we focus the report only on the statistically significant values.

Trust in Government Both trust and distrust of the government correlate heavily with app usage intention. The log odds for both "Somewhat distrust" and "Fully distrust" are proportionally negative compared to the neutral baseline (Log Odds $= -0.56$ and -1.12 respectively). Contrarily, log odds for both "'Somewhat trust" and "Fully trust" are positive compared to the baseline (Log Odds $= 0.81$ and 1.88 respectively).

Worries Of the worries about future health, economy, and social life, only the health scale was included in the final model. All scale points of this scale are significant and show proportional positive log odds compared to the baseline of "No worries about health" (Log Odds in order of rising concern: 0.53, 0.76, and 1.21). This hints at a positive correlation between future health concerns and app usage intention.

Correlation with beliefs As previously reported, we identified many misconceptions. One of them (`(SLF) GOVERNMENT SEES QUARANTINE VIOLATION`) has a negative impact on the installation intention. Two other attributes that also

Factor	Log Odds	C.I.	p-value	
Trust in Government (Q19)				
Trust: Fully agree	1.88	[1.26, 2.50]	< 0.001	$*$
Trust: Somewhat agree	0.81	[0.41, 1.20]	< 0.001	$*$
Trust: Somewhat disagree	-0.56	$[-1.08, -0.04]$	0.035	$*$
Trust: Fully disagree	-1.12	$[-1.85, -0.39]$	0.003	$*$
Beliefs				
`(GEN) THREATS PRIVACY`	$-1,33$	$[-1.82, -0.84]$	< 0.001	$*$
`(GEN) FIGHTS DISEASE SPREAD`	0.55	[0.16, 0.94]	0.005	$*$
`(GEN) RESTRICTS BASIC RIGHTS`	-1.32	$[-1.88, -0.77]$	< 0.001	$*$
`(OTH) GOVERNMENT SEES QUARANTINE VIOLATION`	-0.70	$[-1.08, -0.33]$	< 0.001	$*$
`(SLF) INFORMS MY CONTACTS`	0.51	[0.15, 0.88]	0.006	$*$
`(GEN) MANDATORY USAGE`	0.66	$[-0.07, 1.39]$	0.075	
`(GEN) USES LOCATION SERVICES`	0.42	[0.06, 0.77]	0.022	$*$
`(SLF) DATA TRANSMISSION ONLY AFTER CONFIRMATION`	0.31	$[-0.02, 0.65]$	0.069	
`(OTH) INFORMS IF INFECTED NEARBY`	-0.28	$[-0.61, 0.06]$	0.107	
Worries (Q22)				
Health: Somewhat worried	0.53	[0.04, 1.02]	0.036	$*$
Health: Worried	0.76	[0.24, 1.28]	0.004	$*$
Health: Very worried	1.21	[0.63, 1.79]	< 0.001	$*$
Media Sources (Q7)				
Media: Off. Homepage	0.99	$[-0.14, 2.12]$	0.085	
Media: Publications	0.62	[0.07, 1.18]	0.028	$*$
Media: Public Broadcasters	-0.30	$[-0.63, 0.04]$	0.082	
Personal Experience (Q25)				
Was or knows infected: Yes	-0.06	$[-0.63, 0.51]$	0.840	
Was or knows infected: Don't know	-0.84	$[-1.57, -0.11]$	0.024	$*$
Demographics (Q16, Q18)				
Tech Background	0.24	$[-0.14, 0.62]$	0.208	
Intercepts (App usage intention)				
Definitely not | Probably not	-1.99	$[-2.61, -1.37]$	< 0.001	$*$
Probably not | Undecided	0.35	[0.14, 0.56]	0.001	$*$
Undecided | Probably would	0.53	[0.38, 0.68]	< 0.001	$*$
Probably would | Definitely would not	0.61	[0.48, 0.74]	< 0.001	$*$

TABLE 2.2: Results of the final ordered logit regression model correlating factors with app usage intention. "Don't want to answer" answers were omitted. See Section 2.2.1 and Table A.1 for further details.

negatively correlate with it are attributes that can neither be classified as correct or incorrect but are based on personal sentiment: `(GEN) THREATS PRIVACY` (Log Odds $= -1.33$) and `(GEN) RESTRICTS BASIC RIGHTS` (Log Odds $= -1.32$). `(GEN) USES LOCATION SERVICES` likely is an overestimation of the functionality and correlates positively with the intent to install. Another positive correlating attribute is `(GEN) FIGHTS DISEASE SPREAD` (Log Odds $= 0.55$). Its correctness is hard to measure, as there is no central entity that keeps records of how many people were warned by the app and thus ultimately prevented the spread of COVID-19.

Demographics & Personal Experiences We also were interested in which demographic factors and personal experiences with COVID-19 influence participants' decision to use the CWA. We found a statistically significant effect for

"Not knowing" whether oneself or someone close was infected by COVID-19. There were negative log odds compared to the baseline of not being infected (Log Odds $= -0.84$). This could be due to a "Don't care" (instead of "Don't know") effect.

Potential Properties

As mentioned in Section 2.2.1, we presented the participants different hypothetical statements and consequences of the app (potential properties), asking whether and how that would influence their decision to use it (Q14). Table A.3 in the Appendix shows whether these properties apply to the app as it was described pre-release or not and whether they describe a central or decentral property. We were particularly interested in seeing whether the centralized versus decentralized debate, in which computer scientists and privacy advocates were dominating, was reflected in the broader population's opinions. In the following, we highlight whether the properties belong to the centralized (C) or decentralized (D) approach or if they are independent of the apps' architecture and could be applied to both approaches (B).

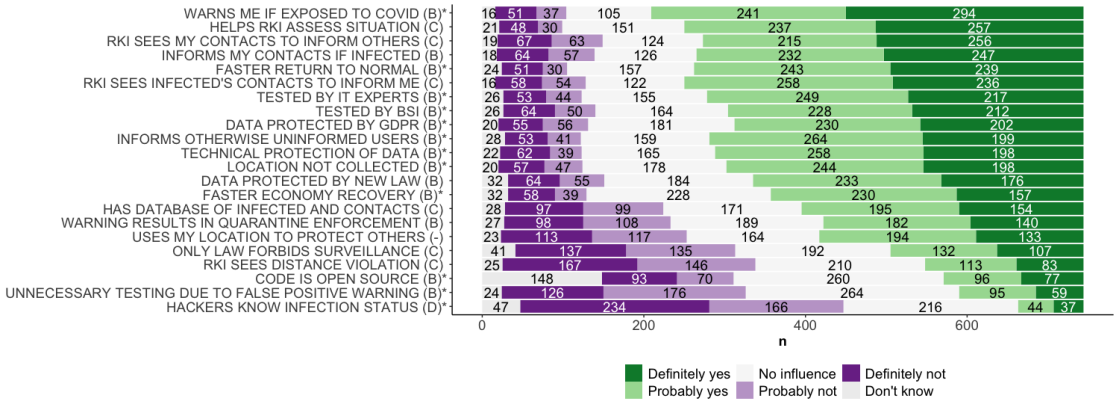


FIGURE 2.7: All presented potential properties and the distribution of the ratings of how these would influence the usage intention. * indicates that they apply to the real app. D = decentralized, C = centralized, B = both, "-" = not included in either app design

Figure 2.7 shows all potential properties and the distribution of how they would influence the participants. It can be seen that no property is rated exclusively positively or negatively.

However, some have a clear negative tendency (i.e., `(PP) HACKERS KNOW INFECTION STATUS`, `(PP) UNNECESSARY QUARANTINE DUE TO FALSE POSITIVE WARNING`), or a clear positive tendency (`(PP) WARNS ME IF EXPOSED TO COVID`, `(PP) HELPS RKI ASSESS SITUATION`).

Usage intention All potential properties were rated from "Definitely would use it" to "Definitely would not use it". The answers of the participants differ visibly based on the previously stated general usage intention of the app as it was going to be released, i.e., participants who stated that they would want to install the app were more positive about all the potential properties than those who stated that they did not want to use the app and vice versa. We tested this observation with Kruskal-Wallis tests. The results show medium to large effects for all 23 potential properties [38]. This means that per property, there is at least one group that differs from the others in their rating. To find out more, we ran pairwise Wilcoxon rank-sum tests and corrected the p-values with a Bonferroni correction. The results can be seen in Table A.5.

The poles ("Definitely will use the app" and "Definitely will not use the app") of the installation intention differ from all other groups for each property. Most but not all of the other group comparisons also show a statistically significant difference.

To assess the impact of each property, we report for each group whether the given answer suggests a positive, negative, or no change for the previously stated general intent to use the app. To clarify, if a participant stated that they wanted to install the to-be-released app, then any potential property that was rated "Definitely would use it", "Probably would be willing to use it" and "No influence on my willingness" would lead to no change in their intention and we summarize that as: "No change". However, for the same group, a property rated as either "Definitely would NOT use it" or "Probably would NOT be willing to use it" could lead to a negative effect on the previously positive attitude. We rated these properties as "negative change". The same goes for participants whose general usage intention was negative. Any negative properties would lead to "no change" while a positive property might lead to a "positive change". Participants who stated they were undecided could be swayed in either direction, so only properties rated with "No influence on my willingness" were rated with "no change", and the others received either a positive or negative rating.

We can see large differences between the usage intention groups (cf. Figure 2.8 and 2.9, also Figure A.3, A.1, and A.2), especially when looking at the poles of the intention: participants who reported to definitely not use the app (Def-No) (Figure 2.8) are seldom really positive about any property. In contrast, participants who reported to definitely use the app (Def-Yes) (Figure 2.9) are seldom very negative about any property. While we can make no causal claims, the polarisation is noteworthy.

To better assess the individual effects of the different potential properties, we built an ordinal regression model based on a combined score of app usage intention and changes in intention due to these properties (cf. Table 2.3). Care needs to be taken when interpreting the regression model. Its intention is to highlight the direction of change as described above. However, since both the dependent and independent variables are non-equidistant and contain very strong poles (definitively use/definitively not use), the log odds should probably be seen as

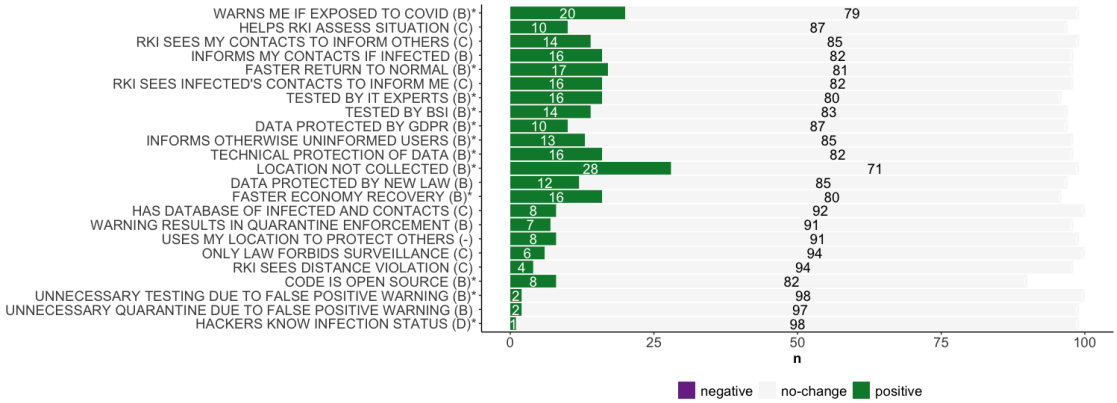


FIGURE 2.8: The figure shows whether potential properties would change their mind for participants who ticked that they would definitely not install the app.

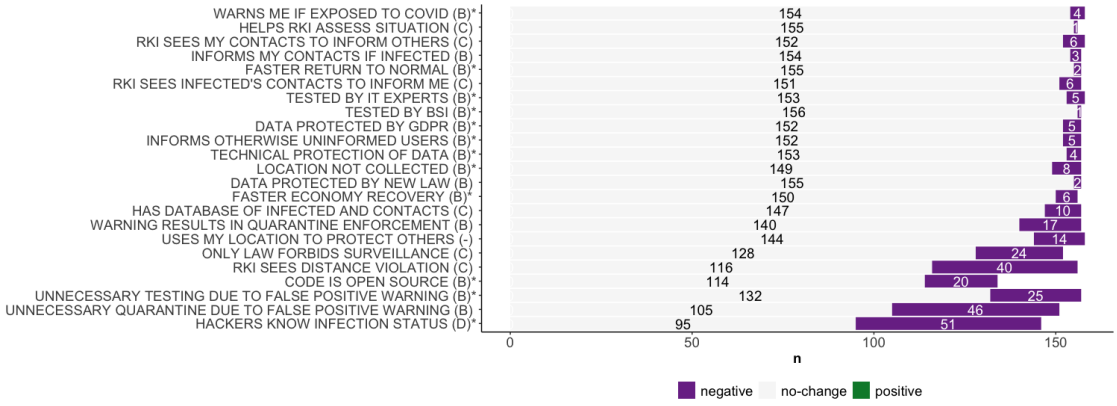


FIGURE 2.9: The figure shows whether potential properties would change their mind for participants who ticked that they would definitely install the app.

an upper bound of the change and need to be used with care.

Twelve of the potential properties apply to the to-be-released app. Nine of those have a positive effect on usage intention, e.g., `(PP) WARNS ME IF EXPOSED TO COVID` (Log Odds = 1.52) and `(PP) INFORMS OTHERWISE UNINFORMED USERS` (Log Odds = 1.01). Both concern the fact that the app would notify users if they could have been at risk of contracting COVID-19. This was the main feature of the app as communicated to the population. Additionally, the intention to install the app increased if it would help returning to a pre-COVID-19 situation: `(PP) FASTER RETURN TO NORMAL` (Log Odds = 1.17) and `(PP) FASTER ECONOMY RECOVERY` (Log Odds = 0.81).

Factor	Log Odds	C.I.	p-value
(PP) WARNS ME IF EXPOSED TO COVID	1.52	[1.31, 1.73]	$< 0.001*$
(PP) INFORMS MY CONTACTS IF INFECTED	1.15	[0.94, 1.37]	$< 0.001*$
(PP) INFORMS OTHERWISE UNINFORMED USERS	1.01	[0.80, 1.23]	$< 0.001*$
(PP) HELPS RKI ASSESS SITUATION	1.28	[1.07, 1.49]	$< 0.001*$
(PP) FASTER RETURN TO NORMAL	1.17	[0.96, 1.39]	$< 0.001*$
(PP) FASTER ECONOMY RECOVERY	0.81	[0.59, 1.03]	$< 0.001*$
(PP) RKI SEES MY CONTACTS TO INFORM OTHERS	1.12	[0.90, 1.33]	$< 0.001*$
(PP) RKI SEES INFECTED'S CONTACTS TO INFORM ME	1.20	[0.98, 1.41]	$< 0.001*$
(PP) HACKERS KNOW INFECTION STATUS	-1.48	$[-1.69, -1.27]$	$< 0.001*$
(PP) RKI SEES DISTANCE VIOLATION	-0.87	$[-1.09, -0.65]$	$< 0.001*$
(PP) USES MY LOCATION TO PROTECT OTHERS	-0.10	$[-0.33, 0.12]$	0.359
(PP) UNNECESSARY QUARANTINE DUE TO FALSE POSITIVE WARNING	-1.34	$[-1.55, -1.13]$	$< 0.001*$
(PP) UNNECESSARY TESTING DUE TO FALSE POSITIVE WARNING	-0.87	$[-1.09, -0.66]$	$< 0.001*$
(PP) WARNING RESULTS IN QUARANTINE ENFORCEMENT	0.04	$[-0.18, 0.27]$	0.709
(PP) HAS DATABASE OF INFECTED AND CONTACTS	0.18	$[-0.04, 0.41]$	0.105
(PP) DATA PROTECTED BY NEW LAW	0.73	[0.52, 0.95]	$< 0.001*$
(PP) DATA PROTECTED BY GDPR	0.88	[0.67, 1.10]	$< 0.001*$
(PP) TECHNICAL PROTECTION OF DATA	1.00	[0.79, 1.22]	$< 0.001*$
(PP) TESTED BY BSI	0.90	[0.69, 1.12]	$< 0.001*$
(PP) TESTED BY IT EXPERTS	1.12	[0.91, 1.33]	$< 0.001*$
(PP) LOCATION NOT COLLECTED	1.10	[0.88, 1.31]	$< 0.001*$
(PP) CODE IS OPEN SOURCE	-0.12	$[-0.34, 0.10]$	0.277
(PP) ONLY LAW PREVENTS SURVEILLANCE	-0.53	$[-0.75, -0.31]$	$< 0.001*$
Neg. change | No change	-1.89	$[-2.05, -1.74]$	$< 0.001*$
No change | Pos. change	1.33	[1.31, 1.35]	$< 0.001*$

TABLE 2.3: Ordered logit regression model correlating different app properties against a combined "Usage Intention Change" scale ranging from 'Negative change" to "Positive change".

Two properties that apply to the app impacted the participants negatively: (PP) HACKERS KNOW INFECTION STATUS (Log Odds $= -1.48$) and (PP) UNNECESSARY TESTING DUE TO FALSE POSITIVE WARNING (Log Odds $= -0.87$). The potential of being exposed by a hacker exists [16], but there are methods to mitigate this threat [90]. The risk for unnecessary testing applies to the app, but this could happen without the app and in both the central and decentral approaches.

Eleven potential properties do not apply to the app, of which five have a statistically significant positive influence on the app usage Three of them belong to the centralized approach and offer the Robert Koch-Institute (RKI) additional insights: (PP) HELPS RKI ASSESS SITUATION (Log Odds $= 1.28$), (PP) RKI SEES MY CONTACTS TO INFORM OTHERS (Log Odds $= 1.12$) and (PP) RKI SEES INFECTED'S CONTACTS TO INFORM ME (Log Odds $= 1.20$). (PP) INFORMS

MY CONTACTS IF INFECTED (Log Odds = 1.15) includes the additional feature of warning users automatically if they had been in contact with an infected person. Currently, users have to actively share their positive test results if they want others to be warned [163].

Three potential properties that do not apply to the app had a negative influence on the installation intention. Two of them ((PP) RKI SEES DISTANCE VIOLATION (Log Odds = −0.87) and (PP) ONLY LAW PREVENTS SURVEILLANCE (Log Odds = −0.53)) open up the possibility of using the app for surveillance and can fall into the centralized approach; one ((PP) UNNECESSARY QUARANTINE DUE TO FALSE POSITIVE WARNING (Log Odds = −1.34)) could be seen as a clear disadvantage for the individual user.

Trust in different entities Some potential properties are connected to measures taken that should build trust regarding the CWA, regardless of the apps' design choices. These measures included different levels of (data) protection by law, experts testing the app, and the possibility to access the code itself.

As can be seen in Table 2.3, the idea to protect the data by a new law ((PP) DATA PROTECTED BY NEW LAW (Log Odds = 0.73)) as well as the existing protection by the GDPR ((PP) DATA PROTECTED BY GDPR (Log Odds = 0.88)) had a positive influence on the intention to use the CWA. Additionally, the technical protection of the data positively influenced the participants ((PP) TECHNICAL PROTECTION OF DATA (Log Odds = 1.00)). However, the participants did not seem to like the idea that the government would only be hindered by law to misuse the data for surveillance ((PP) ONLY LAW PREVENTS SURVEILLANCE (Log Odds = −0.53)).

It was also rated positively if the CWA would be tested by the German Federal Office for Information Security (BSI) ((PP) TESTED BY BSI(Log Odds = 0.9)) and experts ((PP) TESTED BY IT EXPERTS(Log Odds = 1.12)).

Interestingly, unlike the expert discussion would have suggested, (PP) CODE IS OPEN SOURCE did not have a positive effect.

The influence of this property is not statistically significant, and it received the most "I don't know" answers compared to all other properties. Even though the terminology "Open Source" is also used in Germany and was communicated in this way in the press release [215] in order to create transparency and trust, we believe many participants lacked an understanding of "Open Source". It thus does not yet seem to have the positive image the technical community would like it to have.

Perception of location services (PP) LOCATION NOT COLLECTED had a statistically significant positive influence on the installation intention (Log Odds = 1.10). (PP) USES MY LOCATION TO PROTECT OTHERS did not have a significant influence. At the beginning of the survey, we asked participants whether they

believed the CWA would use location services. As a reminder: using the users' position was neither the case for the CWA nor was it communicated at any point. However, as mentioned in Section 2.2.2, the survey question asked about "location services", and Bluetooth may be known as such; therefore, participants could have interpreted it this way. We looked at whether the aspect of location services would make a difference for the installation intention. We compared the participants who a) thought that the CWA would use location services but not Bluetooth to b) those who did not believe the CWA uses location services regarding their general usage intention.

49.8 % of 197 vs 49.7 % of 298.

Usage intention	LBNB belief?	Positive influence if no location usage
Undecided	Yes (n= 46)	26.1%
	No (n= 108)	28.7%
Prob-No	Yes (n= 27)	3.7%
	No (n= 53)	15.1%
Def-No	Yes (n= 25)	4%
	No (n= 65)	7.7%

TABLE 2.4: Percentage of participants who rated the potential property that the app would not collect data about users' position positively based on their general usage intention and whether they believed the app would be working with location data. LBNB = Location service but no Bluetooth.

We then also checked whether participants rated the potential properties more positive if they previously indicated that the CWA would use location services. Table 2.4 shows the percentages of participants who were positively influenced by the property (i.e., answered "Probably would install it" or "Definitely would install it"), split by the general usage intention. As can be seen, the belief that the CWA uses location data did not positively affect the participants' sentiment when being asked how not enabling the government to see their current location would influence them.

2.2.3 Discussion

In the following section, we discuss our results, connect them with previous work, and propose directions for future research.

Participant Beliefs

The majority of the participants knew something about the CWA: Only 5.0% were not able to mark any of the correct app features as true, and the basic idea

behind the CWA (that it would warn users with a risk of infection) was known by 59.5% (see Figure 2.4).

Bluetooth and Location Services We saw a lot of missing information. The technical details that the CWA would use Bluetooth were only known by 43.5%. Interestingly, 30.0% of the participants with some knowledge thought the CWA would use location services but not Bluetooth. While this topic was discussed quite extensively in the media [45, 219], many people did not seem to think that the CWA would do tracing without GPS or the like. We also hypothesize that many who caught the term "Bluetooth" in the debate did not eliminate GPS from their mental model of the CWA. Another element that could get mixed up with information about the CWA might be the use of cellular network data to measure changes in mobility at the population level, as introduced earlier in the year [189]. Interestingly, we did not see any correlation between the assumption that the CWA uses location services and the usage intention.

Infected Persons Nearby 57.5 % of the participants believed the CWA would warn its users if an infected person is nearby. This was also found by Thomas et al. [202], who studied participants' knowledge regarding the already released Australian app and who found 57.4% of their participants believed this. It was also the most common misconception found by Williams et al. [223] (conducted in the UK). This belief seems very common, even if it was never planned nor (to our knowledge) communicated through official channels that the CWA would be able to warn users of infected persons in their vicinity directly. We are unaware of work that provides insight into why people assume this to be true. However, we hypothesize that many people mixed the two possible app features of being warned afterward and being alerted in real-time. With an incorrect understanding of how contacts are captured and in which cases the infection status is sent or downloaded, the belief that the CWA could provide real-time warnings is not too far-fetched and will appear more often throughout this dissertation. Future research should investigate if such vital differences can be communicated, maybe even without going into technical details. It should be noted that this is an overestimation of the CWA's functionality and could lead to incautious behavior based on a false sense of security.

Privacy Concerns 27% of the participants believed the CWA would restrict their basic rights or threats their privacy. These beliefs had significant negative influences on usage intention. Related work found that one of the reasons participants did not want to use an app was because they feared data misuse or surveillance [124, 208]. Some even thought they would receive the names of infected persons [233]. Since the German app (CWA) follows the decentralized approach, only very little data is sent to a central server. While privacy concerns may be valid, we believe many participants did not follow the discussion

enough to understand that data storage criticism only concerned the centralized approach. The decentralized app, which was being implemented, stored very little data centrally. We hypothesize they project the worries around the centralized app onto the decentralized one, even if not all concerns are plausible for this approach. Future research is needed to investigate how old mental models can be updated when the underlying system changes and what influences privacy perception. Although, usage intention does not seem to be driven by knowledge about technical details.

Usage Intention We looked at participants' knowledge and beliefs and how they are connected to participants' intentions to use the CWA. Only two attributes to which a correctness value can be assigned had a statistically significant impact on the participants' willingness to use the CWA. The misconception `(OTH) GOVERNMENT SEES QUARANTINE VIOLATION` had a negative impact, the correct attribute `(SLF) INFORMS MY CONTACTS` a positive one. The belief that one's privacy or basic rights were in danger lowered the willingness significantly. It increased if participants thought the CWA would help fight the spread. These assumptions do not reflect knowledge about the app but are based on personal estimations.

As discussed in Section 2.2.2, `(GEN) USES LOCATION SERVICES` is technically correct in some cases. If participants marked this attribute to be true for the CWA, they were significantly more willing to install the app. Even though the absence of location services as a potential property had a positive influence on using the CWA, participants did not value this absence with a higher usage intention even when previously thinking this would be the case. For this, we have two possible plausible explanations: a) people do not care about location service usage or b) other factors override concerns, e.g., believing in the necessity of the CWA.

Both hypotheses are valuable input for the HCI-community and should be further investigated.

Depending on this, it should be evaluated whether conjoint studies are reliable methods to measure possible acceptance in this domain and how the complexity of reality can be included (i.e., incomplete information or consequential thinking). It seems essential to know the participants' attitudes to the real objective of interest (in our case, the tracing app).

Whether to install the CWA or not seems primarily based on the sentiment of trust and the expectancy of a positive effect. This shows that it is important not only to develop trustworthy technologies but also to communicate their trustworthiness and effectiveness successfully. Technical measures aimed at creating trust do not automatically result in such (e.g., as seen for the CWA's open source property).

Demographic Factors

A study by Utz et al. [208] was conducted at the same time as this study in Germany and can thus be used to compare the results directly. While the authors conducted an experiment about hypothetical apps and how a tracing app could or should be built, we asked about an app that had been officially announced with a detailed description of features and was near launch. We can confirm part of their findings: We found a positive influence on the willingness to use a corona app a) if the opinion on state government was favorable, b) if participants were concerned about their health, and c) return to a normal life are possible due to the app. Participants with privacy concerns were less likely to use the app, which we can also confirm.

Never ever or no matter what

Like in our study, other researchers identified participants who did not like any app, regardless of its design choices [208, 132, 118]. We can confirm this finding. Participants within the Def-No group were mostly negative about any of the presented potential properties. 7.1% did not rate a single presented potential property as a positive change. This is similar to the reported 15-21% by Utz et al. [208]. We also saw the exact opposite: Participants belonging to the Def-Yes group rated every single theoretical additional aspect more positively than all other groups. For all potential properties, participants from the installation intention poles (Def-Yes and Def-No) give statistically significantly different answers compared to all other groups.

Centralized versus Decentralized

Large parts of the discussion around corona tracing apps concerned the technical approach and whether encounters between app users should be stored on a central server or the user's phone. Both approaches come with their advantages and disadvantages. For instance, the centralized app could give the RKI[10] better insights into how people get infected. Since the central database would be in charge of selecting which users need to be warned, the RKI could see how many people are warned per positive case. Since the risk is computed on the users' devices in the decentralized app, the RKI does not know how many people receive warnings. In the centralized app, it would also have been possible to track how many other positive cases come out of any case, potentially giving more insights into how the virus spreads. On the other hand, the decentralized approach does not facilitate getting an overview but is also not in danger of being extended and misused for surveillance. In general, the centralized app,

[10] According to their website, "The Robert Koch Institute (RKI) is the government's central scientific institution [a federal government agency] in the field of biomedicine. It is one of the most important bodies for the safeguarding of public health in Germany." [174]

as it had been planned, offered more insights to healthcare professionals but bore a higher risk of compromise and misuse. However, it is worth noting that the decentralized approach relies on making anonymized infection information public on a central server. This opens the system up for local deanonymization attacks. Suppose an attacker can capture the ephemeral BT-IDs from a target and thus tying those IDs to that target. In that case, they can then monitor the system and see whether they report themselves as positive or not. The German app was based on the decentralized approach due to public pressure to chose a more privacy-preserving approach. So in the context of this study, we were especially interested in how participants rate the possible benefits and dangers of a centralized app and to see if the debate led by researchers and privacy advocates well represented the feeling of the general public. We included 6 potential properties (Q14) in the survey that were connected to the centralized approach (Table A.3).

All in all, we saw a mix of sentiments. Three central potential properties (`(PP) RKI SEES INFECTED'S CONTACTS TO INFORM ME`, `(PP) RKI SEES MY CONTACTS TO INFORM OTHERS`, `(PP) HELPS RKI ASSESS SITUATION`) had a statistically significant positive influence on the intention to install. All three concern individual or societal benefits. Two other central properties (`(PP) RKI SEES DISTANCE VIOLATION`, `(PP) ONLY LAW PREVENTS SURVEILLANCE`) impacted the intention to install negatively. Both focus on the disadvantages of the centralized approach and do not have any clear advantage for the individual user.

The decentral property `(PP) HACKERS KNOW INFECTION STATUS` impacted the participants in a negative way. While this risk is limited to local attackers, and there are methods to mitigate this threat [90], it is something that our participants did not like. However, it did not feature significantly in the public debate as far as we know and, as such, is unlikely to have had much of an impact.

It seems participants are in general inclined to rate properties of the centralized approach positively while they rate the consequences (in the current technical landscape) that come with it rather low.

In summary, many of our participants had very positive views concerning the increased capabilities the centralized app would have had. This suggests that there could have been more support in the population for a more feature-rich app than academics and privacy advocates acknowledged in the discussion preceding the CWA's publication. Relevant health officials have since stated that the app in its current form is no great support [54], and due to the privacy design, it is hard to evaluate its efficacy. We think it is worth discussing whether a more nuanced discussion about the feature/privacy trade-off would be warranted for the future.

2.2.4 Conclusion

We surveyed the usage intention of the CWA in Germany right before its launch. 50% of the participants reported their intent to use the CWA, 26.3% refrained

from usage and 23.4% were undecided. To understand the participants' decision, we investigated what beliefs they had about the CWA. We saw many false beliefs, especially concerning technical details, i.e., 30.0% of the participants thought the CWA would use location services (other than Bluetooth). Actual knowledge about the CWA does not seem to be the primary driver for the decision to use the CWA. Instead, perceived privacy or basic rights intrusions led to a lower intention to use it. As also reported by other researchers, we found a positive effect when people were worried about general health and trusted the government. We also highlight that the general population's views were more diverse and more open to a central entity getting an overview to help fight the pandemic than the public discussion indicated. Based on our results, we recommend future work on a) where the privacy concerns come from, as in our view, many of the concerns did not match the actual CWA and b) how the perceptions can be aligned with the actual facts of the CWA, as this is necessary to discuss features based on the facts. At last, we recommend working on c) whether the CWA can be extended in a way that it becomes more useful to the relevant parties, e.g., the public health departments, while at the same time implementing technical countermeasures to prevent the data from being abused.

2.2.5 Acknowledgements

We thank, in alphabetical order: Yomna Abdelrahman, Ruba Ali Mahmoud Abu-Salma, Florian Alt, Zinaida Benenson, Nataliia Bielova, Freya Gassmann, Katharina Krombholz, Mattia Mossano and Melanie Volkamer for their insightful discussions and helpful remarks on the survey. This work was partially funded by the Werner Siemens Foundation.

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

Disclaimer: The contents of this chapter are based on the published paper "Less About Privacy: Revisiting a Survey about the German COVID-19 Contact Tracing App," presented at the 2023 CHI Conference on Human Factors in Computing Systems. The paper was written by my co-authors, Eva Gerlitz, Christian Tiefenau, and Matthew Smith and me. The paper received an "HONORABLE MENTION" award. As this work was conducted with my co-authors as a team, this chapter will use the academic "we" to mirror this fact. I led the analysis of the quantitative data, supported by Christian Tiefenau, after designing the study with my co-authors. I managed the analysis of the qualitative data done by Christian Tiefenau, Eva Gerlitz, Julia Angelika Grohs, and me. Finally, I led the compilation of the results and their presentation for publication. Before compiling the paper for publication, all authors jointly discussed the study's implications.

As reported in Section 2.2, we found that even though the German government followed the more privacy-preserving decentralized approach after public discussions [47], 27.4% of the participants considered the app to be a threat to their privacy. Besides this, participants had many misconceptions about the app. Half the participants reported they had some intention of installing the app. The study had been conducted before the app's release, so we could only gather statements about intended future behavior and beliefs about an app that was not yet available.

As intended and actual behavior tend to show a gap in several research areas [179], 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 survey study presented in Section 2.2 with minor adaptations in August 2020, two months after the release of the app in June. Again, we conducted our study with a quota sample of the German population ($n = 837$).

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 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 sections are structured as follows: In Section 2.3.1, we provide a short overview of the malfunctions of the German contact tracing app (CWA). In Section 2.3.2, we describe our methodology, especially compared to the original study. Section 2.3.3 presents the results of the replication in comparison to the original one. Finally, in Section 2.3.4, we discuss our findings and provide directions for future work.

2.3.1 Context and Related Work

In this section, we provide an overview of the malfunctions of the CWA and other studies on the development of knowledge and misconceptions about contact tracing apps over time. Finally, we will give an overview of what is called the "intention-behavior gap".

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) [89]. 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 [230] and iOS [195]. 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 [230]. 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 [88]. 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 [192].

Besides these, several minor issues, such as unhelpful error messages, were brought up by public broadcasters [231] or discussed on GitHub [86, 87, 85].

Knowledge Before and After the Apps' release

One of our goals with this study was to look at how peoples' knowledge developed over time.

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

Kozyreva et al. [126] 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. [143] were in line with this. In a one-off survey study of (non-)users, they found that knowledge about the app features positively relates to app usage.

A study by Munzert et al. [148] 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, contrasting to what Meier et al.'s [143] results may allow to hypothesize.

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 [5, 179]; 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 [179, 6]. While different studies and topics show different sizes of the gap, Sheeran et al. [179] 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 a complex 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 [179]. People also face challenges when they want to act on an intention, e.g., people often forget to act or miss opportunities [179].

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., [76, 160, 10]), or understanding peoples' interaction with technical devices (e.g., [62]).

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. Theoretical or (soon-to-be) existing apps were then examined, 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. [217], varied between studies and countries in the range of 38%-84%. Acceptance rates in Germany seem to lie in between: Kostka et al. [124] reported an acceptance rate of 41%, we were able to report 50%, and Altmann et al. [9] reported 60%.

However, Kozyreva et al. [126] 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. [115] 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. [148] and Kozyreva et al. [126]. Jamieson et al. [115] 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. [179] 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 [179]. 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.

2.3.2 Methodology

Our methodology follows that of the previous one (see Section 2.2), with minor changes in the questionnaire, as explained below.

Survey Content

We reused the survey that was designed before the app was released; so we adjusted all tenses and answers accordingly. Details are described in the following paragraphs.

Screening The 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).

Media Sources and Knowledge We asked the participants about their sources of information about the app (Q7[11]), 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.

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. Now, they could also indicate that they had uninstalled it or were planning to install it. We then asked for the primary reason (Q13).

Previous Survey It was not possible to recruit the same participants as in the previous study, 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 the 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).

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.

Potential Properties The survey had 24 statements of potential properties of the app and asked the participants 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.

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

Recruitment

We followed the same recruitment process as before: Using Qualtrics [168], we aimed to draw a representative German sample according to age, education, household income, and residence (federal state). For this, we used the same

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

quotas as before. 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.

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 [207] based on the free text answers. If this was not possible, the qualification was set to "undefined."

Analysis

We followed the analytical approach of the previous study to describe the participants' knowledge and their reported intention to use the app, respectively, and, 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 gathered for Section 2.2 and `cwa_beh` for the data gathered in this 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 ($n = 6$).

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.)[12] 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

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

many demographic characteristics). As testing everything for differences did not seem a sensible option, we omitted further inferential statistics.

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. [208] 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. [208] 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. [208] needed to be expanded. The final code book is shown in Table 2.7 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 [64]; the documents were selected randomly, as suggested by O'Connor and Jeffe [152]). We used ReCal3 [72] 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, 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, these 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 [71]. 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.

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.

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 [148]. Third, we set the same quotas as in the previous study, but just like in that study, the recruitment by Qualtrics did not match them 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 2.5). 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 first study. Therefore, a

direct comparison of intention vs. behavior per participant was not possible. To compensate for this, we worked with a large quota sample.

2.3.3 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.

Demographics

		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	**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
AFFILIATION (Q24)	**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 2.5: Participants' demographics ($n = 837$), in percentages. Gray: Percentages from `cwa_int` ($n = 744$). Numbers in brackets represent the targeted distribution [168, 63].

The participants were recruited as described in Section 2.3.2. 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 2.5.

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 [217]. 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 B.1 and B.2, which show the detailed numbers of the participants based on their socio-demographics.

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 B.1.

Knowledge about the app increased Despite the divisive nature of the many COVID-19 measures [188] and the disinformation targeted at them [234, 214], it is nice to see that knowledge about the app increased while misconceptions declined. In the study described in Section 2.2 9.89% of the participants correctly checked every point mentioned in the official press release regarding the app. 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 2.3.1, not actively opening the app

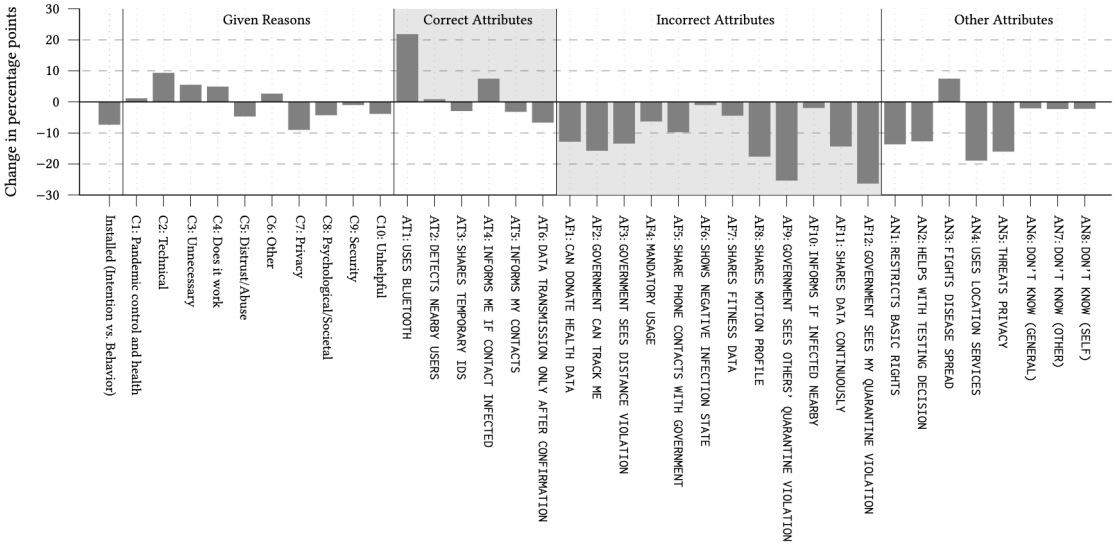


FIGURE 2.10: Gains and losses in p.p. of **high-level codes**, **attributes**, and **app installation intention and action**. If a bar is in the area with a gray background, more participants in `cwa_beh` than in `cwa_int` had correct knowledge about this specific attribute. We can see this is the case 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.

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., [27]) 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%).

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 (to 11.4% and 6.4% respectively).

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 [155].

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 [13], 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."

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.

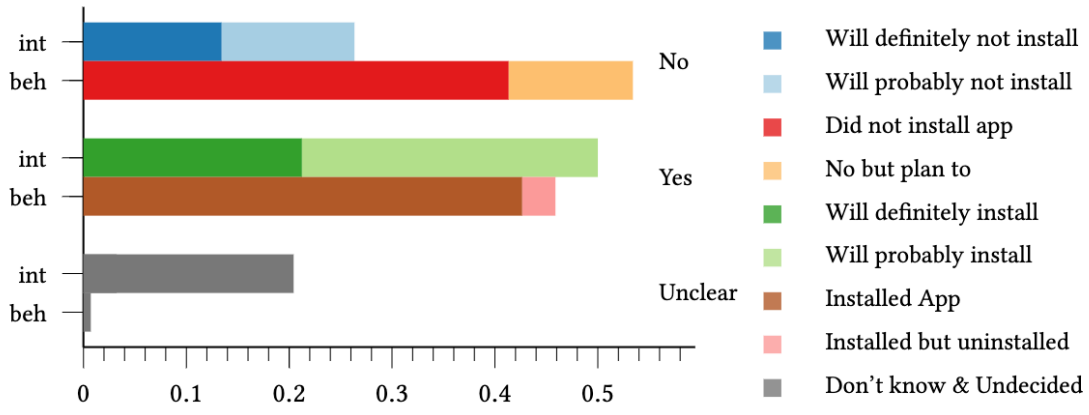


FIGURE 2.11: Installation intention (int) as reported in `cwa_int` vs. installation behavior (beh) as reported in `cwa_beh`.

Figure 2.11 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 installed 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 [48])[13], which translates to 28.98% of the smartphone users in Germany (60.74 Mio., based on an estimation from 2020 [186]). 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.

Influence of Knowledge on App Installation In Section 2.2 we 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 Table 2.6.

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

	CWA_int				CWA_beh			
Factor	**Log Odds**	**C.I.**	***p*-value**		**Log Odds**	**C.I.**	***p*-value**	
(Q23) Trust in Government								
Trust: Fully agree[B]	1.88	[1.26, 2.50]	< 0.001	$*$	1.45	[0.73, 2.18]	< 0.001	$*$
Trust: Somewhat agree[B]	0.81	[0.41, 1.20]	< 0.001	$*$	0.68	[0.17, 1.19]	0.008	$*$
Trust: Somewhat disagree[B]	-0.56	$[-1.08, -0.04]$	0.035	$*$	-0.62	$[-1.32, 0.08]$	0.085	
Trust: Fully disagree[B]	-1.12	$[-1.85, -0.39]$	0.003	$*$	-1.20	$[-2.64, 0.25]$	0.105	
Beliefs								
`USES BLUETOOTH`[B]					1.13	[0.72, 1.55]	< 0.001	$*$
`THREATS PRIVACY`	$-1,33$	$[-1.82, -0.84]$	< 0.001	$*$	-4.50	$[-7.49, -1.51]$	0.003	$*$
`INFORMS MY CONTACTS`	0.51	[0.15, 0.88]	0.006	$*$	0.86	[0.38, 1.34]	< 0.001	$*$
`SHARE PHONE CONTACTS WITH GOVERNMENT`[B]					-2.97	$[-4.77, -1.17]$	0.001	$*$
`MANDATORY USAGE`[B]	0.66	$[-0.07, 1.39]$	0.075		3.73	[0.80, 6.66]	0.013	$*$
`GOVERNMENT SEES MY QUARANTINE VIOLATION`[B]					-1.20	$[-2.14, -0.27]$	0.012	$*$
`DATA TRANSMISSION ONLY AFTER CONFIRMATION`	0.31	$[-0.02, 0.65]$	0.069		0.52	[0.12, 0.91]	0.011	$*$
`SHOWS NEGATIVE INFECTION STATE`[B]					0.49	[0.07, 0.90]	0.023	$*$
`SHARES MOTION PROFILE`[B]					-0.55	$[-1.05, -0.05]$	0.031	$*$
`GOVERNMENT SEES DISTANCE VIOLATION`	-0.98	$[-1.92, -0.04]$	0.042	$*$				
`SHARES FITNESS DATA`	1.75	$[-0.42, 3.91]$	0.114					
`CAN DONATE HEALTH DATA`	0.36	$[-0.13, 0.85]$	0.147					
`FIGHTS DISEASE SPREAD`	0.55	[0.16, 0.94]	0.005	$*$				
`RESTRICTS BASIC RIGHTS`	-1.32	$[-1.88, -0.77]$	< 0.001	$*$				
`GOVERNMENT SEES OTHERS' QUARANTINE VIOLATION`	-0.70	$[-1.08, -0.33]$	< 0.001	$*$				
`USES LOCATION SERVICES`	0.42	[0.06, 0.77]	0.022	$*$				
`INFORMS IF INFECTED NEARBY`	-0.28	$[-0.61, 0.06]$	0.107					
Worries								
Health: Somewhat worried	0.53	[0.04, 1.02]	0.036	$*$				
Health: Worried	0.76	[0.24, 1.28]	0.004	$*$				
Health: Very worried	1.21	[0.63, 1.79]	< 0.001	$*$				
Media Sources								
Media: Gov. Websites[B]					0.71	[0.32, 1.11]	< 0.001	$*$
Media: Off. Homepage[B]	0.99	$[-0.14, 2.12]$	0.085		1.83	[1.00, 2.65]	< 0.001	$*$
Media: Private Broadcasters					-0.33	$[-0.74, 0.08]$	0.117	
Media: Publications	0.62	[0.07, 1.18]	0.028	$*$				
Media: Public Broadcasters	-0.30	$[-0.63, 0.04]$	0.082					
Personal Experience								
(Q30) Knows deceased person	Baseline: Yes							
No[B]					-2.20	$[-4.11, -0.29]$	0.024	$*$
Don't know[B]					0.03	$[-3.08, 3.14]$	0.985	
(Q28) Risked person close	Baseline: No							
Yes					0.70	[0.27, 1.12]	0.001	$*$
Don't know					0.49	$[-0.38, 1.36]$	0.271	
(Q29) Was or knows infected	Baseline: No							
Yes	-0.06	$[-0.63, 0.51]$	0.840					
Don't know	-0.84	$[-1.57, -0.11]$	0.024	$*$				
Demographics								
(Q24) Party	Baseline: CDU/CSU							
AfD					-0.36	$[-1.40, 0.67]$	0.492	
Others/Don't want to state					0.57	$[-0.05, 1.19]$	0.072	
The Left					-0.19	$[-0.84, 0.46]$	0.566	
FDP					-0.91	$[-1.84, 0.02]$	0.054	
The Greens					0.20	$[-0.34, 0.74]$	0.464	
SPD					-0.64	$[-1.24, -0.04]$	0.037	$*$
(Q20) Gender: Female					-0.53	$[-0.92, -0.14]$	0.008	$*$
Tech Background	0.24	$[-0.14, 0.62]$	0.208					
Intercept					-0.33	$[-2.42, 1.76]$	0.758	
Definitely not | Probably not	-1.99	$[-2.61, -1.37]$	< 0.001	$*$				
Probably not | Undecided	0.35	[0.14, 0.56]	0.001	$*$				
Undecided | Probably would	0.53	[0.38, 0.68]	< 0.001	$*$				
Probably would | Definitely would	0.61	[0.48, 0.74]	< 0.001	$*$				

Table 2.6: Regression Models of cwa_int (Ordered Logistic Regression) and cwa_beh (Logistic Regression, $R^2 = 0.414$). If factors also occurred in the cwa_beh-model based on BIC, they are marked with [B]. The largest negative effect size in both sets is that participants felt threatened in their privacy.

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.

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 2.7.[14] A visualization of the increase and decrease is included in Figure 2.10. 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 B.2.

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

Code	% in data set (installation status per code in %): `cwa_int` (✓, unclear, ×)	`cwa_beh`	ICR_int	ICR_beh	Example
C1: Pandemic control and health [208, 108, 126, 143]	**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[148, 208, 108, 14]	**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 [208, 108]	**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 [208, 108, 148, 14, 126]	**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 [148, 208, 14]	**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[148, 208, 108]	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 [108]	-	1 (0, 0, 100)	-	undef*	"Have always put it off until now"
C7: Privacy [148, 208, 108, 14, 69, 9, 204, 126]	**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 [208, 108]	**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) [9, 143]	0.7 (100, 0, 0)	0.1 (100, 0, 0)	1	undef*	"Sounds credible and developers are known"
C9: Security [208, 9]	**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 2.7: 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.

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 B.1, 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.

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 2.3.1.

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.

2.3.4 Discussion

We revisited a survey study shortly after the release of the German contact tracing app, the Corona-Warn-App (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.

Privacy and Ideological Reasoning

When the original survey was conducted, the apps' privacy was a big issue. In April 2020, organizations dealing with internet politics (including the "Chaos Computer Club"[37] and the "Gesellschaft für Informatik" [111]) 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 [46].

Arzt et al. [14], 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 [208, 126, 9]. In `cwa_int`, 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. 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. [148] 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 [28, 96]). 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 [112]. 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. [115]).

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% in `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. [208], e.g, used the IUIPC, Seeberger et al. [177] the MUIPC, and Jamieson et al. [115] 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. [127] 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. [127], 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 [137], and thus, it is hard to assess what notion of privacy (e.g., informational, interactional, or social [137]) 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. [208], 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 Participants Were Certain About Their Decision What did remain constant between the original study and our replication was the absolute certainty of participants. The title of the previously published paper presented in Section 2.2 [101] 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.

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. [9] 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 [200], 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 [200, 107]. 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. [21] 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. [137]). 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. [21].

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 [86, 87, 85]. 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.

Lesson Learned from Replicating an Intention Study

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. [126] and Munzert et al. [148] (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 [185], but we cannot say for sure how exactly this relates to the installation numbers. Contrary to the numbers previously reported by us (see Section 2.2), Kozyreva et al. [126], and Munzert et al. [148], Kulyk et al. [127] 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. [115] 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. [115]. 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.

Age Related work found a contradictory influence of participants' age. While Altmann et al. [9] found younger participants more willing to install a contact tracing app, the literature also offers the opposite finding [217, 148].

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 B.1). 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 [19]. While it might be challenging, we strongly encourage researchers to actively recruit older participants for such studies.

2.3.5 Conclusion

We repeated the survey study presented in Section 2.2 about the Corona-Warn-App (CWA) 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.

2.3.6 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.

2.4 I have not understood but agree. Studying informed consent in the context of the German COVID-19 contact tracing app

Disclaimer: At the time of this work, the basis of the chapter's contents is under review as part of the paper "I have not understood but agree. Studying informed consent in the context of the German COVID-19 contact tracing app" at the ACM Transactions on Computer-Human Interaction (TOCHI). This was joined work together with Eva Gerlitz, Christian Tiefenau, Felix Kretschmer, Alina Stöver, and Nina Gerber. As this work was conducted with my co-authors as a team, this chapter will also use the academic "we" to mirror this fact. Initially, Felix Kretschmer conducted and analyzed interviews as part of his final thesis for his master's degree. They were the basis on which Eva Gerlitz, Christian Tiefenau, Alina Stöver, Nina Gerber, and I designed the survey. I was not involved in the design nor the analysis of the interviews, but for better understandability and readability of the presented survey study, I provide the corresponding text parts in Appendix C.3. Nina Gerber did the statistical tests on the survey data, which were later analyzed by Nina Gerber and me, and before being compiled for publication, the results were discussed with Christian Tiefenau and Eva Gerlitz.

In the two previous studies, we learned that the participants had different ideas about how the CWA works. Even though in the second study, more participants knew that the app uses Bluetooth or that the app is intended to warn its users, there were also some misconceptions that clearly misjudged the app's capabilities. Ideally, people should neither underestimate nor overestimate the app. The app should not give a false sense of security, but neither should it raise unnecessary concerns because users agree to use it under their assumptions. That a user uses an app under the right assumptions can be subsumed under the term informed consent, a term also utilized by the General Data Protection Regulation (GDPR).

In this chapter, however, we understand the term more broadly than the GDPR defines it. We mean that a person is not only informed but that this information has also been accepted and processed.

Research has provided evidence that many users lack this crucial knowledge in other areas than Contact Tracing App (CTA)s [138, 92, 121, 153, 120, 73].

The CWA used new technology, both novel and important to the general public. The technological details are complex, so although users can understand it in principle, it can be assumed that most citizens initially had very few matching intuitions of how the technology works. As already mentioned multiple times privacy, and with it how the CWA handles data, has taken a central role in German media, reporting on the app as well as public campaigns advertising to use the app [196, 84, 129, 65, 56].

Adding to existing studies on CTAs, e.g., [208, 60, 177], our goal was to examine the assumptions held by citizens – both app users and non-users – regarding

the collection and processing of their data in the CWA. This investigation additionally aimed to determine if the usage of the app could be considered as under informed consent. Based on an interview study (cf. Appendix C.3), we designed a survey and formulated the following research questions:

RQ1: Do the mental models of data collection and processing differ between users and non-users of the CWA? Previous studies have revealed that users of existing CTAs possess more knowledge about the apps compared to non-users [126, 143]. However, these studies have primarily examined specific elements of the apps, such as the use of Bluetooth, mobile, or location data [126], or have focused their analysis on the influence of knowledge on usage [143]. Our research aimed to delve into the depth of knowledge possessed by participants based on their usage of the CWA.

RQ2: Do mental models of data collection and processing differ between citizens with high privacy concerns and those with low privacy concerns? Privacy concerns were found to have a negative impact on the installation intention [208], yet educating participants about the app's data privacy only indicated small effects on installation rates [148]. We sought to determine whether concerns about a specific app are isolated to that app or reflect a general sentiment held by individuals. Additionally, we aimed to investigate whether this sentiment is rooted in or influenced by an understanding of the technology. Therefore, we measured the general sentiment with the Internet Users' Information Privacy Concerns (IUIPC) and tested for a knowledge difference in the groups.

To address these questions, we conducted a survey study (N = 352) to examine common themes identified in the interviews (cf. Appendix C.3) and analyze potential differences between the assumptions of CWA users and non-users (RQ1), as well as people with high and low privacy concerns (RQ2).

The survey data confirm the trend of the previous Sections. There seem to be various ideas regarding the collection and processing of data, as well as data accessibility during the process. However, overall, users tend to possess a better understanding of these concepts compared to non-users. Participants who previously used the app but later uninstalled it exhibited a similar level of understanding as current users, albeit with less confidence in the app's ability, especially in maintaining their anonymity. Despite this, the impact of usage status on mental models of data collection and processing was small, with both users and non-users harboring several misconceptions. Furthermore, our data indicated a correlation between privacy concerns, as measured by the IUIPC-8 [141, 93], albeit small ones, and the accuracy of participants' understanding of the app's operations. Participants with higher Awareness and Control scores tended to have a more accurate understanding of the app's functionality in comparison to those with fewer concerns. In conclusion, it is evident that a non-negotiable number of participants do not possess a correct understanding of the basic principles of data collection and processing within the app. Hence, we are contributing to the discussion regarding whether decisions are based on facts and the applicability of informed consent in the context of CTAs, as well as in a broader sense.

The remainder of this section is structured as follows: in Section 2.4.1, we present an overview of related work specifically relevant to the survey. Section 2.4.2 details the methodology, and Section 2.4.3 details the survey study's results. Our findings are discussed in Section 2.4.4.

2.4.1 Context and Related Work

In this section, we provide a historical context of the pandemic situation in Germany during the survey, as well as a summary of relevant work related to our research questions. All of our research questions aim to address the underlying question of whether individuals are able to give their informed consent to the functions of the app when choosing to install it. In order for informed consent to be granted, individuals' mental models must, at least partially, align with technical facts.

Background: Pandemic Situation in Germany

In this section, we summarize the pandemic situation in Germany for September 2022, the time period during which the survey was conducted.

The first case of COVID-19 in Germany was reported at the end of January 2020 [194]. In response, in March of that year, Germany implemented measures, such as schools closures, border restrictions, and the closure of non-essential shops to curb the spread of the virus [193].

In September 2022, the Omicron BA.5 variant had become the predominant strain in Germany [169], resulting in infection rates ranging from 200 to 500 per 100,000 people[173]. Despite this, the numbers remained relatively low compared to the previous winter when rates exceeded 1000 cases per 100,000 people[173]. Around three-quarters of the population had received their basic immunization, with a significant portion having also received their first booster vaccination by this time [104].

In September 2022, the German parliament approved new COVID-19 regulations for the upcoming autumn and winter seasons. One of the key measures included the mandatory use of FFP2 masks in public transportation (long-distance) and medical facilities. Additionally, individual federal states were given the authority to enforce mask-wearing in other settings, such as events and short-distance public transportation [30].

As of September 2022, the app had been downloaded 47 million times [136]. However, it is important to note that the number of downloads does not necessarily equate to the number of active users. To estimate the active user base, the CWA team analyzed backend data and information on active devices in app stores. Their findings in February 2022, with 43 million downloads, indicated that the CWA had between 25 and 31 million [81] active users, representing approximately 30 to 37% of the German population [25].

Data Protection, Knowledge and Informed Consent

According to the GDPR, obtaining informed consent is a mandatory requirement when collecting and processing personal data, whether fully or partially automated (unless there are other compelling reasons as outlined in Article 6) [66]. The European Commission defines informed consent as follows: "Informed consent means that you must be given information about the processing of your personal data, including at least:

- the identity of the organisation processing data;
- the purposes for which the data is being processed;
- the type of data that will be processed;
- the possibility to withdraw consent (for example by sending an email to withdraw consent);
- where applicable, the fact that the data will be used solely for automated-based decision-making, including profiling;
- information about whether the consent is related to an international transfer of your data, the possible risks of data transfers to countries outside the EU if those countries are not the subject of a Commission adequacy decision and there are no adequate safeguards." [39]

Research in the areas of privacy policies, app permissions, and cookies has revealed obtaining informed consent is oftentimes a challenge. Users frequently do not read privacy policies and terms of service thoroughly, if at all [153]. If they would it could be a very time-consuming task [142]. Additionally, these documents are often complex and difficult to understand, especially for people without post-graduate education [116]. Hence, although the GDPR emphasizes the importance of providing information with users, from an HCI perspective, it becomes clear that true consent requires more than merely making the information available. Instead, users must actively notice and (correctly) understand the information presented to them in order to truly make *informed* decisions.

Another substantial issue in data protection arises from the potential conflict between users' privacy needs and the interests of service providers. A study by Harbach et al. [98] found that when users are informed about the implications of app permissions, they tend to make more privacy-conscious choices. Current implementations of cookie consent notices often fail to empower users to make meaningful decisions or even nudge them towards less privacy-friendly options [92, 149, 138, 209]. This is compounded by the fact that users' expectations regarding rules of data protection are not always aligned with the reality of legislation [58].

We contend that the dilemma described in the case of the CWA is not applicable. Despite the privacy policy being lengthy [80], the CWA was developed

with a minimal data approach in mind [82], prioritizing trust through transparency [83]. Therefore, the service provider had a strong incentive to be as open as possible and educate users, believing that transparency would drive adoption. Efforts were made to convey this message through extensive advertising and public communication focusing on the principles of privacy-preserving, data-minimalism, and transparency [22, 78, 129]. We, thus, consider the CWA to be successful in *providing* the necessary information for obtaining information on data handling. Still, we question whether simply providing this information translates into people being genuinely *informed* in practice, i.e., whether they understand the provided information, including the identity of the data processor, purposes of data processing, types of processed data, and possible transfer of the collected data. We understand this question to be decoupled from the legal perspective, i.e. whether and how the app achieves the consent required for GDPR compliance.

Relation of Knowledge and Installation status

Our first research question asks whether users are differently informed than non-users. The existing literature suggests that people who have installed a CTA or plan on doing so are better informed than those not using or intending to use it. For instance, Kozyreva et al. [126] discovered that while 65% of app users knew the German app used Bluetooth, only 26% of the non-users were aware of this fact. Meier et al. [143] also found that knowledge about the app's privacy features positively related to app usage. Participants from the two studies presented in Section 2.2 and Section 2.3 were more likely to be willing to install the CWA or to have it already installed under the correct assumption that the app would inform the user's contacts if they tested positive for SARS-CoV-2 and knew that an authority had to confirm a positive test result before it could be shared over the app. In Section 2.3, users' awareness of the app using Bluetooth correlated with having the app installed.

Additionally, Alharbi et al. [8] reported that older adults in Saudi Arabia refrained from installing a CTA due to their lack of understanding of the technology. Participants from the two studies presented in Section 2.2 and Section 2.3 who believed the government could potentially use the app for surveillance purposes (e.g., by receiving phone contacts of users or seeing violations of distancing or quarantine rules) were statistically less likely to install or have it installed. Interestingly, the misconception that the app could be used to prove a non-infection status (with regard to the app's functionalities at the time of the study) was associated with higher rates of app installation (cf. Section 2.3).

While the literature suggests a correlation between app installation and knowledge about the app, there is a lack of strong evidence for a causal relation. On the contrary, we found literature that provides evidence for a non-causal relation. Acquiring knowledge about the apps does not necessarily lead to installing them, as a study by Munzert et al. [148] indicates: participants who were taught

about an app indeed had increased knowledge and positive attitudes toward the app, but the uptake numbers did not rise.

Privacy Concerns and Knowledge

Several studies, as detailed in an overview by Gerlitz et al. [77], have shown that participants who are concerned about their privacy in relation to contact tracing are less likely to consider installing such an app or have it already installed. In Section 2.2, we allowed participants to express their beliefs regarding a specific app (the CWA) and gauged their sense of privacy threat by inquiring about their perceptions of certain statements related to the app. Several of these statements could be seen as actual threats to users' privacy (e.g., whether the government can see the user's location data). Yet, participants were not asked whether they viewed these statements as privacy concerns. We found an interesting situation: more participants believed two incorrect statements about the app than those who considered it a privacy threat. Specifically, participants believed that the app shares a motion profile and notifies users of nearby infected individuals. While these beliefs could be seen as significant privacy issues, not all individuals who held these beliefs viewed the app as a threat to their privacy. Consequently, the relationship between privacy concerns and app knowledge remains ambiguous, making it challenging to pinpoint the underlying reason for people's apprehensions.

These concerns may stem from personal attitudes rather than factual knowledge. Instruments like the IUIPC [141] can measure such personal attitudes. Previous research has linked IUIPC scores to the intention to install an CTA [208], but, to the best of our knowledge, no studies have explored the connection between privacy concerns, personal attitudes, and knowledge about a specific app. Therefore, we incorporated the IUIPC into our survey study and formulated our second research question accordingly.

Trust

Studies found that trust in the country's government or politics in general leads to a positive influence on the intention to use an app [148, 34, 208]. Conversely, distrust in stakeholders or difficulty in understanding COVID-19-related regularities leads to citizens being less likely to install the CTA [15, 208]. Furthermore, it was observed that trusting science also leads to higher uptake in installation rates [34]. Velicia-Martin et al. [213] utilized an extended technology acceptance model (TAM) to measure participants' intention to install the app, finding a link between trust in the app and the intention to use it.

Therefore, to cover that aspect, we included the scale by Gulati et al. [95] to measure the participants' trust in the CWA.

2.4.2 Methodology

In an interview study (cf. Appendix C.3), we identified topics related to assumptions and concerns regarding the app. They found that the themes were prevalent in both groups: users and non-users. To quantify the prevalence of these topics on a larger scale and their distribution within these two groups (users and non-users, RQ1), we conducted a survey study with 151 users, 151 non-users, and 50 past users. Based on themes from related work, we also included privacy concerns (IUIPC-8, RQ2) as additional differentiating variables.

In this section, we describe our methodology.

Survey Creation

Since our goal was to quantify the prevalence of assumptions and concerns with regard to the CWA that were identified in the interviews, we created questions that cover the different assumptions in the presented mental models and the various concerns raised by the interview participants. Statements from their interview participants were used as answer options. If the list of answers was incomplete or missed the correct answer, these options were added. This evaluation of completeness was executed using our own knowledge about the CWA and results from related work (e.g., [148, 126]). During the interviews (cf. Appendix C.3), not all participants differentiate between encounters with other CWA users and infection statuses. As the technical handling of encounter data and infection status is, in fact, very different, we decided to split the two concepts into different blocks but ask otherwise, where applicable, identical questions so that it is possible to identify participants who do not distinguish between them. In related work [202, 223], it seemed that participants believed that the CWA had some "real-time warning" of infected people in the vicinity. To investigate further whether this belief is actually present or if the questions might have been misinterpreted, we included two specific questions (Q23l and Q23b, see S13 in Table C.3).

Most knowledge questions were asked in the following form: "To what extent do you believe the following statements are true?" and could be answered by a 7-point Likert scale ranging from 1 = "Strongly agree" to 7 = "Strongly disagree". We also added the option "I do not know" but asked participants to only use this if they had no assumption at all. Questions were shown in random order where applicable. Following the knowledge questions, the participants were presented with an explanation of how the CWA works, which only focused on the most important features to ensure the attention of the participants (see Figure C.1). We then asked the participants for their trust in the CWA. For this, we used the scale as given by Gulati et al. [95].

The final survey can be found in Appendix C.1 and included the following topics (the Qx notation refers to the question number):

1. Consent

2. Screening question and demographics (Q1-Q5)

3. Installation status of the CWA (Q6) (Here we wanted to distinguish between users, non-users, and former users of the CWA)

4. Involved actors (Q7,Q8), data collection (Q9), data use (Q12), and access (Q10, Q11) to collected data

5. Encounter data: Collection (Q13, Q14), access (Q15), storage (Q16, Q17), transfer (Q18a, Q18b), anonymity (Q18c)

6. Infection status: Access (Q20), storage (Q22), transfer (Q21b, Q21f), anonymity (Q21a, Q21c, Q21g), and warnings (Q21d, Q21e)

7. Further knowledge apart from encounter data and infection status (Q23b, Q23c, Q23e, Q23g, Q23j, Q23l)

8. Questions concerning the capabilities of and the perception toward the app (Q23a, Q23d, Q23f, Q23h, Q23i, Q23k, Q23m)

9. Trust in the CWA and public information (Q25 [95], Q24)

10. Usage of app features (Q26, Q27) (Here we wanted to know which of the different features offered by the CWA (e.g., encounter notifications and risk calculation, contact journal, storage of vaccination certificate) were currently or previously used by the participant

11. Dark triad personality traits [117, 140] (Q28)

12. Privacy concerns IUIPC-8 [141, 93] (Q30)

Used questionnaires The IUIPC-8 [93, 141] measures individuals' general privacy concerns, i.e., privacy concerns that are always prevalent and not related to the use of a specific application or technology. It includes three scales: (1) Awareness - someone with high Awareness scores aims to be well informed about the collection of their data, (2) Control - someone with high Control scores aims to exercise control over how their data is handled, (3) Collection - someone with high Collection scores believes that the collection of data alone is a privacy violation, regardless of the circumstances.

The scale developed by Gulati et al. [95] contains 12 items and assesses user trust in the interaction with systems. The influencing factors here are (1) Perceived Risk, (2) Benevolence, and (3) Competence.

Survey Testing

We conducted pilot tests with four participants, whom we recruited from our personal contacts, who were not part of creating the survey. We asked them to share their thoughts with us while answering the survey. Three of the pilot participants used the CWA and one was a former user. We refined the survey based on the feedback and our own observations.

Recruitment and Participants

For our research questions, we performed a power analysis to calculate the number of participants required to detect an effect we would be interested in (d = 0.5, considered a medium effect [38]) for Mann-Whitney U tests. Although related work suggests that users might be better informed than non-users, we refrained from one-tailed tests due to the small sample sizes. Further, we had no assumptions to specify a hypothesis regarding privacy concerns. Hence, we decided to conduct a two-tailed, requiring a sample size of 67 participants per group to reach a power of 0.8. We aimed to split the sample into two parts, below the 25% and above the 75% percentiles, for the analysis of RQ2, hence, we needed at least 268 participants. However, because participants had the option to select "I don't know" for most statements, we could not estimate with certainty how many participants the data set would contain for each statement. Therefore, we decided to recruit a total of 350 participants to be on the safe side.

We used Clickworker [36] to recruit 350 participants between September 5th and 8th, 2022. We posted two separate studies in Clickworker to specifically target (1) users and (2) non-users to ensure an equal number of participants in both samples. Participants needed to indicate on Clickworker that they live in Germany to be invited to the study. Participants received €2.46 for their participation, which equals the minimum wage in Germany at the time of the study for 15 minutes. In the end, the median participation time was 14 minutes.

Participants had to own a smartphone that is able to run the CWA, as we assumed that people who did not have the opportunity to install the CWA were less likely to be interested in its functionality and technical details and, thus, should not be expected to possess detailed knowledge about it.

Due to a technical issue, we received two additional complete answer sets. Hence, our sample includes 352 participants. A total of 26 participants did not pass at least one of the attention checks. They were then excluded during the answer phase and did not appear in the final sample provided by Clickworker. For the survey participants' detailed demographics, please refer to Table 2.8. A total of 151 participants used the app at the time of the study, while 151 participants had never used it.

	Age	Gender	Education	IT Security Experience	IUIPC [93]		
					Awareness	Control	Collection
Users (N=151)	M=40.34 SD=12.42 min=18 max:76	Women=42% Men=57% Non-binary=1%	None=1% Some high school=1% High school=9% A levels=19% Bachelor's degree=19% Master's degree=25% PhD=5% Apprenticeship=21% Other=0%	None=90% <2 years=5% 2-5 years=4% >5 years=1%	M=5.91 SD=1.17 ≤25%=5 ≥75%=7	M=5.40 SD=1.20 ≤25%=4.5 ≥75%=6.5	M=5.24 SD=1.30 ≤25%=4.5 ≥75%=6.3
Non-users (N=151)	M=39.59 SD=11.82 min=18 max=71	Women=36% Men=63% Non-binary=1%	None=0% Some high school=1% High school=9% A levels=23% Bachelor's degree=17% Master's degree=29% PhD=1% Apprenticeship=19% Other=1%	None=92% <2 years=5% 2-5 years=1% >5 years=1%	M=5.89 SD=1.24 ≤25%=5 ≥75%=7	M=5.34 SD=1.29 ≤25%=4.5 ≥75%=6.5	M=5.34 SD=1.43 ≤25%=4.3 ≥75%=6.8
Past users (N=50)	M=41.08 SD=14.41 min=21 max=70	Women=32% Men=68% Non-binary=0%	None=0% Some high school=4% High school=12% A levels=28% Bachelor's degree=6% Master's degree=28% PhD=2% Apprenticeship=18% Other=2%	None=82% <2 years=2% 2-5 years=4% >5 years=12%	M=6.19 SD=1.09 ≤25%=5.9 ≥75%=7	M=5.43 SD=1.42 ≤25%=4 ≥75%=6.6	M=5.26 SD=1.29 ≤25%=4.5 ≥75%=6.3
Total (N=352)	M=40.13 SD=12.44 min=18 max=76	Women=38% Men=61% Non-binary: 1%	None=0.3% Some high school=1% High school=10% A levels=22% Bachelor's degree=16% Master's degree=27% PhD=3% Apprenticeship=20% Other=1.7%	None=90% <2 years=5% 2-5 years=3% >5 years=3%	M=5.94 SD=1.19 ≤25%=5 ≥75%=7	M=5.38 SD=1.27 ≤25%=4.5 ≥75%=6.5	M=5.29 SD=1.05 ≤25%=4.5 ≥75%=6.5

TABLE 2.8: This table presents the survey participants' demographics. We had as many users as non-users and a third group of past-users that we didn't explicitly recruit but categorized based on their answers (Q6).

Another 50 participants reported having used the app in the past but did not use it at the time of the study[15]. Upon a closer look at the data distribution, we found that these participants can neither be assigned to the users nor non-users but display a distinct answer pattern. We decided to include them in the analysis as a third group. Based on our power analysis, the sample size of the past user group is too small to reach a power of 0.8 for medium-sized effects.

[15]One part of past users appeared in the first dataset and one part of past users appeared in the second dataset

Thus, our analysis might have failed to detect existing effects for this group. Still, we included our findings to provide a starting point for future research.

Analysis

Due to the ordinal scale level of our data, we used non-parametric tests (i.e., Kruskal-Wallis and Mann-Whitney U tests with Bonferroni-Holm correction to account for multiple testing) to explore our research questions. Since there is no established scale for capturing the mental models of data collection and processing of the CWA, we followed the usual recommendations for the scale development process [145]: first, we generated items based on the existing literature, following which we tested these items on selected individuals. Subsequently, we used exploratory factor analysis (EFA) and internal consistency measures (Cronbach's alpha) to check the mapping of items to scales. Specifically, we conducted an EFA using maximum likelihood as extraction criteria with varimax rotation to assess the relationship between the items. Here, the goal was to identify the factors underlying the items, i.e., in some cases, several items capture the same overarching construct. For example, the items "Information about the CWA is provided openly and honestly by official bodies (e.g., the German government" (Q24a) and "The officially published information (e.g., from the German government, RKI) about the CWA is correct" (Q24b) both measure whether participants believe that official information about the CWA is true. This is reflected in the results of the EFA, which groups items based on how participants responded to those items (these groups are called factors) and to which extent the individual items match those factors (this is called factor loadings). If multiple items are considered to measure the same factor, they were summarized to a *scale* by calculating the average of the individual item responses for each participant and then proceeding with this averaged scale value in the analysis. Based on the factor loadings (see Figure C.5) and reliability analysis (for which we used Cronbach's alpha), we created 27 scales. For this, we considered which items have high factor loadings on the same factor. We only grouped items that refer to the same construct content-wise. For example, the items capturing whether one's identity can be assigned to one's infection status (Q21a, Q21c, Q21g) and encounter data (Q18c) had high factor loadings on the same factor, but we decided to create two separate scales: one referring to the infection status (S3: Identity can be assigned to infection status) and another to encounter data (S4: Identity can be assigned to encounter data) as we wanted to consider both beliefs separately. Due to the same considerations, we did not group the items inquiring about the data collected within the CWA (Q9), and the items questioning who had access to the location data (Q10), demographic information (Q11), encounter data (Q15), and infection status (Q20). Additionally, we only grouped such items to a scale that have a high internal consistency (measured via Cronbach's α). For the factor loadings and Cronbach's α values for all items and scales, please refer to Table C.3 in Appendix C.1. To test for differences

between participants with low and high privacy concerns (RQ3), we compared participants below the 25 and above the 75 percentiles. The proportion of users, past users, and non-users is displayed in Table 2.9. The full statistics of the tests can be found in the Appendix in Table C.1, C.2, and C.4.

	PC Awareness	PC Collection	PC Control
Users	≤25%: 41 (44.1%) ≥75%: 54 (39.1%)	≤25%: 45 (41.7%) ≥75%: 36 (37.9%)	≤25%: 45 (41.7%) ≥75%: 42 (41.2%)
Past users	≤25%: 9 (9.7%) ≥75%: 23 (16.7%)	≤25%: 16 (14.8%) ≥75%: 10 (10.5%)	≤25%: 17 (15.7%) ≥75%: 17 (16.7%)
Non-Users	≤25%: 43 (46.2%) ≥75%: 61 (44.2%)	≤25%: 47 (43.5%) ≥75%: 49 (51.6%)	≤25%: 46 (42.6%) ≥75%: 43 (42.2%)
Total	≤25%: 93 (100%) ≥75%: 138 (100%)	≤25%: 108 (100%) ≥75%: 95 (100%)	≤25%: 108 (100%) ≥75%: 102 (100%)

TABLE 2.9: The table shows how users, past users, and non-users are distributed among the privacy concerns ≤25% and ≥75% percentiles. The percentiles are used to test for differences in assumptions about the CWA (RQ3).

Ethics

The study was reviewed and approved by our institution's Research Ethics Board, and we adhered to the German data protection laws and the GDPR in the EU. Prior to the survey, the participants were informed about the purpose of the study and provided their consent to the data being used for research. Throughout the survey, they were offered the option to not answer any question and allowed to drop out at any time without any consequences.

The survey was implemented via Qualtrics [168]. We anonymized the answers, thus Qualtrics did not store IP addresses and location data in the survey results. Participants were informed and subsequently gave their consent to their data's storage, as it would be stored on servers from Qualtrics as well as computers and servers from involved researchers.

Limitations

We recruited the participants over Clickworker, which likely shifts our sample to a younger and technically more capable sample compared to the general population in Germany. COVID-19 and political measures to fight it (including the CWA) were, and still are, topics that brought up a lot of emotions. Since the purpose and subject of the study were clearly stated in the invitation of our study, people who were annoyed by COVID-19 in general or do not believe in its existence might not have followed the invitation, as a study by Munzert et al. indicates [148], further shifting our sample. Further, we lacked the sufficient power to analyze the effects for the group of past users. Thus, we might have failed

to detect existing differences between past users and users/non-users. Further research is needed to explore this user group in more detail.

The functionality of the CWA is, in part, quite complex. Thus, we needed to simplify the technical details for the questions without oversimplifying them, introducing some imprecision to the questions and therefore potentially the answers.

We conducted the survey late in the pandemic, in September 2022. While shortly after the CWAs release, many media news covered the app and technical details, this was not the case anymore at the time of the study. Participants might have forgotten, or never aware, about technical details they knew when they installed the app. To ensure adequate inclusion of all participants, we offered the option "I don't know."

2.4.3 Results

In the following subsections, we describe our results. This section describes the survey results. Initially, we provide a descriptive analysis of the responses from the participants and present the findings in relation to the research questions. To aid in comparison and easy location of information, the subsequent sections and corresponding figures will employ a uniform structure. We only report differences between groups if they are statistically significant with $p<.05$. The results of the pairwise comparisons are displayed in Table 2.10.

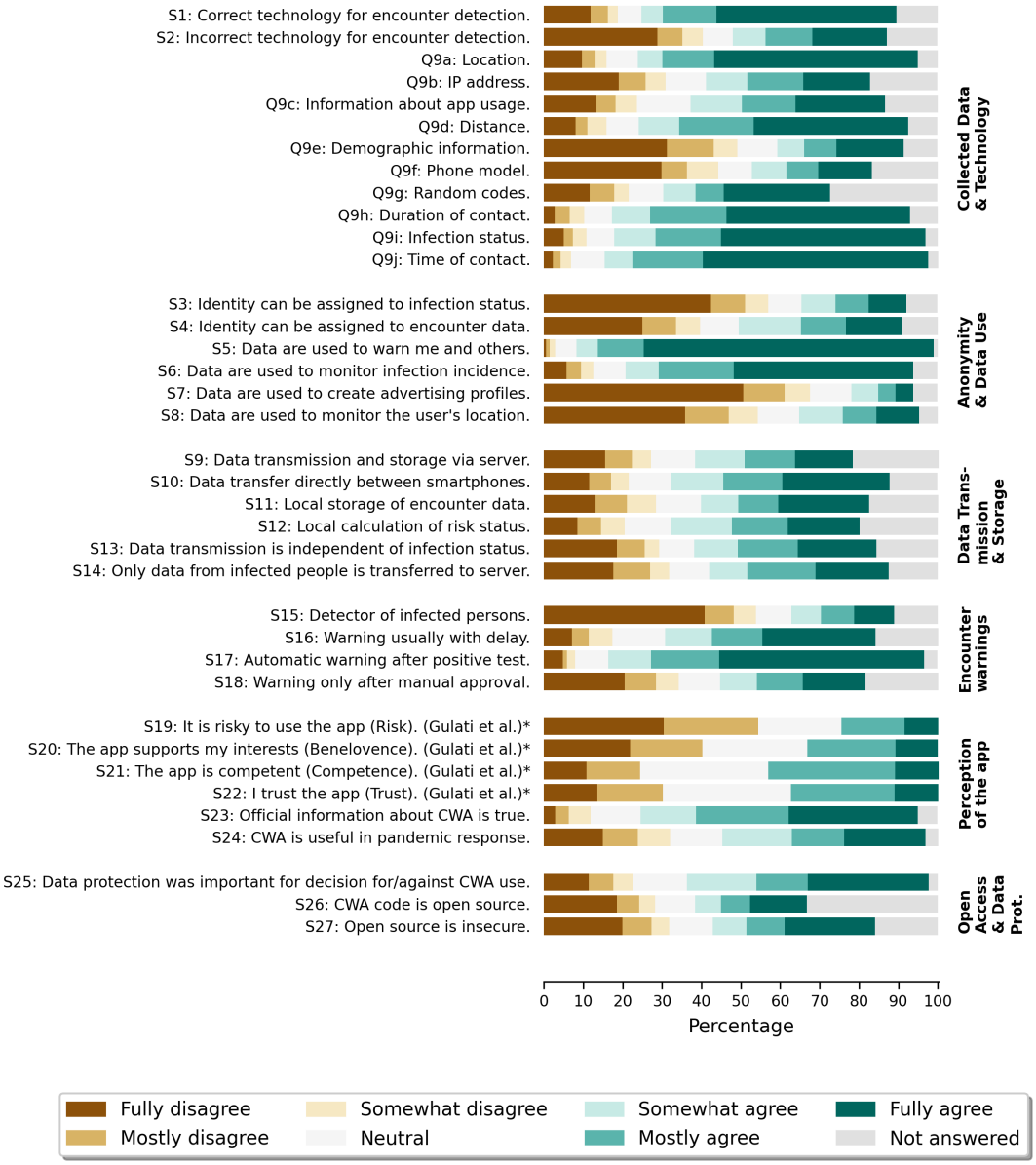


FIGURE 2.12: Answers to statements covering various assumptions the participants had about the CWA (anonymity, data use, technology, data transmission, data storage, warnings). Items marked with * were asked on a 5-point scale. They missed the "mostly disagree" and "mostly agree."

Descriptive

This section provides an overview through descriptive statistics of the participants' knowledge and assumptions. It describes our sample and sets the baseline for the analysis of the research questions. We sorted the questions and scales into seven categories that describe different aspects of the CWA's functionality. For each reported statistic, we reference the scale or question used.

Collected Data and Technology After more than two years availability most participants correctly assumed that the app would capture the time they had encountered other app users (82%, Q9j), the duration of this contact (76%, Q9h), and their infection status (79%; see Figure 2.12, Q9i). However, most participants also thought that the app would store their location (71%, Q9a). Half of our participants indicated that they either thought no random code would be captured (22%, Q9g) or that they were not aware of this (27%, Q9g). About two-thirds of our participants agreed with the correct statement of the app using Bluetooth for detecting encounters (65%, S1), while about 31% (S2) of the participants tended to assume that the app uses another technology for this purpose, e.g., GPS, mobile data, satellite, or WiFi.

Anonymity and Data Use Roughly an equal number of participants ($\sim$40%, S3) assumed that their identity could or could not be matched to their encounter data, while a slightly higher number of participants (57%, S4) thought that their identity could not be matched to their infection status (see Figure 2.12). Overall, most participants were not afraid of data misuse and thought that their data would only be used to warn others (91%, S5) and monitor the infection incidence (73%, S6). Most participants indicated that they thought their data would not be used to monitor their location (54%, S8) and create advertising profiles (68%, S7).

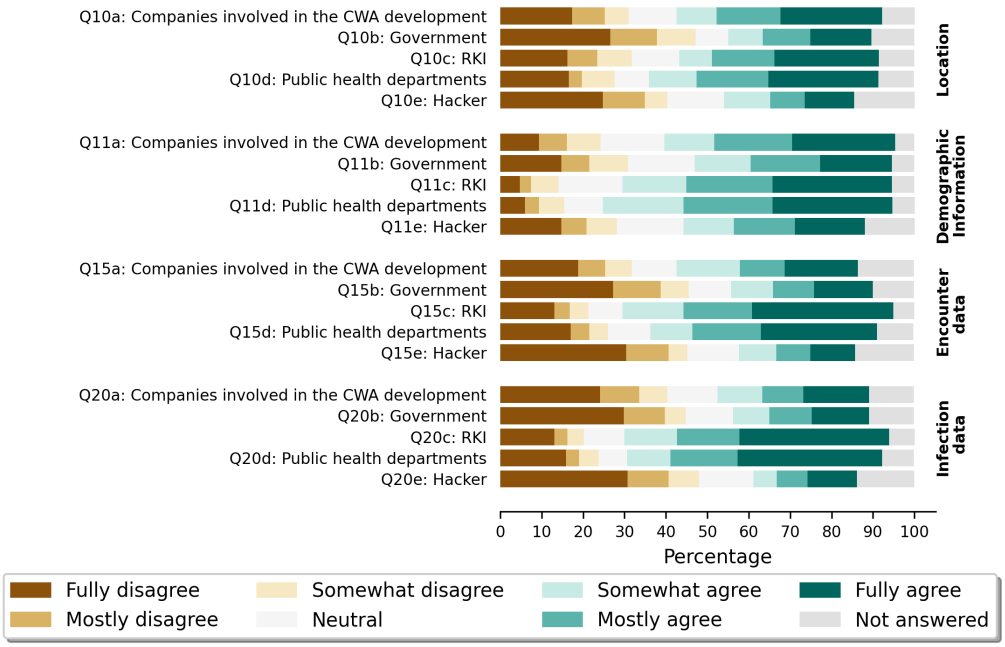


FIGURE 2.13: Answers to statements covering various assumptions the participants had about who had access to the data participants assumed the CWA gathered

		Users vs. Non-Users	Users vs. Past Users	Past Users vs. Non-Users	Privacy Concerns (≤25% vs. ≥75%) Awareness	Collection	Control
Collected Data & Technology	S1: Correct technology for encounter detection [Bluetooth]	↑ .23**		↑ .25**	↓.16*		↓.16*
	S2: Incorrect technology for encounter detection	↓.26**					
	Q9a: Location	↓.16**		↓.21**	↓.32**	↓.21**	
	Q9b: IP address	↓.19**					
	Q9c: Information about app usage	↓.22**		↓.23**		↓.16*	
	Q9d: Distance to others	↑ .16**			↓.15*		↓.16*
	Q9e: Demographic information	↓.30**		↓.19*			
	Q9f: Phone model				↑ .19**		
	Q9g: Random code	↑ .17*					
	Q9h: Duration of contact	↑ .16**			↓.26**		↓.15*
	Q9i: Infection status				↓.35**	↓.14*	↓.20**
	Q9j: Time of contact				↓.31**	↓.20**	↓.23**
Anonymity & Data Use	S3: Identity can be assigned to infection status	↓.30**	↓.17*		↑ .25**		↑ .21**
	S4: Identity can be assigned to encounter data	↓.22**					
	S5: Data is only used to warn others				↓.55**	↓.30**	↓.41**
	S6: Data is used to monitor infection incidence				↓.28**	↓.19**	↓.16*
	S7: Data is used to create advertising profiles	↓.20**			↑ .32**		↑ .23**
	S8: Data is used to monitor the user's location	↓.29**		↓.20**	↑ .19**		↑ .18*
Data Transmission & Storage	S9: Data transmission and storage via server					↓.15*	
	S10: Data transfer directly between smartphones						↓.17*
	S11: Local storage of encounter data	↑ .16*	↑ .20*				
	S12: Local calculation of risk status	↑ .17*					
	S13: Data transmission is independent of infection status	↓.19**					
	S14: Only data from infected people is transferred to server						
Data Access	*Access to location data (Q10)*						
	a: Companies involved in the CWA development	↓.16*				↓.21*	
	b: Government	↓.21**			↑ .16*		↑ .21*
	c: RKI	↓.21**					
	d: Public health departments	↓.20**					
	e: Hacker	↓.24**					
	Access to demographic information (Q11)						
	a: Companies involved in the CWA development						
	b: Government						
	c: RKI				↓.27**		
	d: Public health departments				↓.29**		↓.28**
	e: Hacker					↓.27*	
	Access to encounter data (Q15)						
	a: Companies involved in the CWA development	↓.17**		↓.17*			
	b: Government				↑ .16*		↑ .19**
	c: RKI				↓.14*		
	d: Public health departments						
	e: Hacker	↓.33**					
	Access to infection status (Q20)						
	a: Companies involved in the CWA development	↓.24**		↓.20**			
	b: Government				↑ .17*		↑ .22**
	c: RKI	↓.18**			↓.14*		
	d: Public health departments	↓.18**					
	e: Hacker	↓.30**		↓.18*			
Encounter warnings	S15: Detector of infected persons	↓.26**		↓.24**	↑ .18**		↑ .22**
	S16: Warning usually with delay	↑ .20**			↓.16*		↓.20**
	S17: Automatic warning after positive test				↓.35**	↓.22**	↓.27**
	S18: Warning only after manual approval		↑ .26**				
Perception of the app	S19: Risk *Gulati et al. [95]*	↓.43**	↓.22**	↓.17*		↓.17*	
	S20: Benevolence *Gulati et al. [95]*	↑ .33**	↑ .30**		↑ .13*		
	S21: Competence *Gulati et al. [95]*	↑ .43**	↑ .26**				
	S22: Trust *Gulati et al. [95]*	↑ .45**	↑ .36**				
	S23: Official information about CWA is true	↑ .33**	↑ .21**		↓.24**		↓.30**
	S24: CWA is useful in pandemic response	↑ .49**	↑ .39**				
Open Access & Data Prot.	S25: Data protection was important for deciding				↓.24**	↓.42**	↓.16*
	S26: CWA code is open source						
	S27: Open source is insecure	↓.21**					

*Note. *p<.05, **p<.01, ***p<.001 after correction for multiple testing.*

TABLE 2.10: This table shows the results of Mann-Whitney-U-tests comparing the scales resulting from our analysis covering various mental model concepts (anonymity, data use, technology, data transmission, data storage, warnings) of users, past users, non-users, and participants with low (≤25%) and high (≥75%) privacy concerns (PC). Only statistically significant differences are reported with their effect size r. The effect sizes are represented by three gray values (small effect $r < 0.3$ as light gray, medium effect $0.3 < r < 0.5$ as medium gray, and large effect $r > 0.5$ as dark gray). The direction of the effect is indicated by an arrow: For example, a ↑ in the "Users vs. Non-Users" column signals that users scored higher on the respective scale than non-users, a ↓ means that non-users scored higher than users. In the Privacy Concerns columns, a ↑ indicates that participants with low (≤25%) privacy concerns scored higher than participants with high (≥75%) privacy concerns, and a ↓ indicates that participants with high (≥75%) privacy concerns scored higher than participants with low (≤25%) privacy concerns. The corresponding questions for each concept represented by a scale can be seen in Table C.3, for the Z-values of the tests, look at Figure C.4.

Data Transmission and Storage More participants thought their encounter data (55%, Q16c) and infection status (57%,Q21f) were transferred directly between smartphones than via a server (encounter data: 38% (Q16b); infection status: 43% Q21b). Likewise, the number of participants who believed that their encounter data was stored only locally (43%, S11) and their risk status was calculated locally (48%, S12) was greater than the number of participants who thought that this was done on a server (encounter data: 41%, Q16d; risk status: 37%, Q23g). A slightly higher number of participants tended to agree with the incorrect statement that the transfer of their data is independent of their infection status (46%, S13) than with the correct statement that only the data of infected persons is uploaded to a server (45%, S14). In general, responses were fairly evenly distributed across the different scale points, indicating that the participants held a wide range of assumptions regarding this procedure.

Data Access Regardless of the type of data, including data that was never gathered by the CWA, most participants assumed that the government-associated public health departments (61% location [Q10a], 74% demographic information [Q11a], 60% encounter data [Q15a], 67% infection status [Q20a]) and the RKI (53% location [Q10c], 69% demographic information [Q11c], 69% encounter data [Q15c], 68% infection status [Q20c]) could gain access to their data, followed by the companies involved in developing the app (54% location [Q10b], 59% demographic information [Q11b], 51% encounter data [Q1ba], 41% infection status [Q20b] ; see Figure 2.13). Interestingly, the participants thought it was less realistic that the government itself could gain access to their data (39% location [Q10e], 50% demographic information [Q11e], 38% encounter data [Q15e], 37% infection status [Q20e]) than the previously mentioned parties. Less than half of our participants believe that hackers can gain access to their data (37% location [Q10d], 50% demographic information [Q11d], 33% encounter data [Q15d], 29% infection status [Q20d]).

Warnings about encounters with infected people Most participants (80%, S17) assumed that other users they previously met would be warned automatically once they had entered a positive test result in the app. However, about one-third of the participants (37%, S18) also tend to correctly agree that warnings are sent after a positive test result only after users have manually given their consent. More than half of the participants (53%, S16) also accurately stated that warnings are usually sent with a delay. Still, about one-third of the participants (33%, Q23b) reported that they could tell directly via the app if an infected person was standing next to them. Further, 20% (Q23l) of our participants at least somewhat agreed with the statement that infected persons are shown on a map. This misconception was found much more frequently in past studies, such as Thomas et al. [202] and in Section 2.2.

Perception of the app To measure how the app is perceived by the participants, we used the scales proposed by Gulati et al. [95]. The responses indicated that the participants tend to assume that it is not risky to use the app (54%; see Figure 2.12, S19). Additionally, more participants (44%, S21) tend to assume that the app is competent in its task (i.e., contact tracing) than incompetent (24%, S21), while opinions regarding benevolence and trust toward the app are mixed. Furthermore, we asked two additional questions, the answers indicate that more participants trust the information officially disseminated about the CWA is true (70%, S23) than think it is not (12%, S23), and another question about the usefulness of the app for pandemic containment. For the latter, the participants' responses varied widely (see Figure 2.12), yet more participants thought the app useful (51%, S24) than not (28%, S24).

Open Access and Importance of Data Protection A third of our participants (33%, S26) stated they did not know if the app's code was published under an open-access license (see Figure 2.12, S23-S26). The remaining answers are distributed roughly equally on both sides of the scale, i.e., half of the remaining participants tend to agree that the app code is available as open source (28%, S26)), whereas the other tends to disagree (28%, S26)). However, a slightly higher number of participants agree (41%, S27) than disagree (32%, S27) with the statement that releasing the code under an open-source license would lead to security problems. Feeling that open-sourcing the app would make it less secure is the opposite perception of what was hoped to be achieved by making the development transparent. In total, 61% (S25) of our participants indicated that data privacy played an important role in their decision (not) to use the app, with half of them (31%) strongly agreeing with this statement. Less than a quarter (23%) marked that data protection did not play an important role in their decision. The rest of the participants were indifferent to this question (14%) or said they did not know the answer (2%).

Summary The participants reported a mix of correct and incorrect assumptions, e.g., many assumed that users' locations were somehow gathered. The app was rated rather positively, but again, not by everyone. The incorrect assumptions seem to be often overestimating the amount of data gathered and who has access to it.

RQ1: Do mental models of data collection and processing differ between users and non-users of the CWA?

A possible reason for knowledge differences among the participants might be attributed to whether they are using the CWA. Hence, we hypothesized (RQ1) that users knew more than non-users.

We were interested in whether users had a more accurate view of how the CWA works than past users or non-users. Non-users being unaware of every

detail about the app may not be desirable but understandable. Users, on the other hand, should know at least the basics to be considered informed. We ran statistical tests to see whether we could detect relevant differences between the three groups. We only report differences between groups if they are statistically significant with $p < .05$. Since RQ1 targets three groups (users, past users, non-users), we used Bonferroni-Holm-corrected alpha-levels for the post-hoc tests. The Bonferroni-Holm-corrected alpha-levels for the users, past users, and non-users are .05, .025, and .0167 respectively. The results of the pairwise comparisons with a visualization of the effect sizes are displayed in Table 2.10.

Collected Data and Technology Overall, users seem to have a much better understanding of the data collected than non-users: significantly more users than non-users correctly indicated that the app captures random codes (Q9g), their distance to others (Q9d), and the duration of contact with others (Q9h). Conversely, significantly more non-users than users or past users falsely assumed that the app would assess their location (Q9a), demographic information (Q9e), or information about how they use the app (Q9c), and more non-users than users further think that the app would capture their IP address (Q9b).

Regarding the technology that is used to capture encounters, users and past users tended to agree significantly more frequently to the correct answer option than non-users, i.e., Bluetooth (S1). Incorrect options such as GPS, WiFi, or satellite, on the other hand, were chosen more frequently by non-users (S2).

Anonymity and Data Use We discovered that substantially more non-users and past users compared to users thought that their identity could be assigned to their infection status (S3). Our analyses could only partially replicate the effect we saw for the infection status for encounter data (S4); we saw that significantly more non-users than users indicated that an assignment of their encounter data to their identity could occur. Our analyses further indicate that non-users are particularly afraid of data misuse: significantly more non-users thought that their data would be used to create advertising profiles (S7) and monitor their location (S8).

Data Transmission and Storage Users are significantly more likely than past users and non-users to think that encounter data are stored only locally (S11) and considerably more likely than non-users to think that the risk status is also calculated locally (S12). Non-users are also more likely to assume that their infection status and encounter data will be stored permanently than users. However, users are also significantly more likely than non-users to believe that the transmission path of their data is independent of whether they are infected or not (S13).

Data Access The assumption that the government has access to the user's location via the CWA is significantly more frequent among non-users than users (Q10b). Non-users are more likely than users to think that third parties could access their data, e.g., companies involved in the development or operation of the CWA have access to their data (location Q10a, encounter data, Q15a, infection status Q20a). In line with believing that involved companies can access the app's data, non-users are also more likely to think that hackers would have access to their data (location Q10e, encounter data Q15e, infection status Q20e).

The government-affiliated RKI and public health departments are also more likely to have data access in the view of non-users (location Q10c&d, infection status Q20c&d).

Warnings about encounters with infected people Unsurprisingly, users seem to better understand how warnings are implemented in the app than non-users. For example, they are more likely to agree with the correct statements that warnings are delayed (S16) and they must manually agree in advance to warn people they have encountered if they import a positive test result (S18). Non-users, on the other hand, are more likely to falsely assume that they are warned directly when an infected person is near them and even that they are shown on a map (S15).The results are somewhat more ambiguous with regard to past users: although they have a better understanding than non-users of the fact that warnings are delayed and infected people are not displayed on a map, they are less likely than users and non-users to think that they have to manually agree to warnings being sent if they test positive.

Perception of the app Users have a significantly more positive perception of the CWA than non-users and past users, as evidenced by considerably higher values for benevolence (S20), trust (S18), and competence (S21). Furthermore, users are also more likely to feel that the information disseminated by official channels concerning the CWA is accurate (S23) and that the app makes a meaningful contribution to the pandemic response (S24). Non-users, on the other hand, feel that using the CWA is riskier than users and past users, with the latter again considering it riskier than current users.

Open Access and Importance of Data Protection Non-users are more likely than users to think that publishing the code (open source) would make the app less secure (S27). Our analyses showed no significant differences in the importance of privacy in deciding whether to use the app between users, former users, and non-users (S25) or whether they assume the code to be open source (S26).

Summary We saw that users more often recognized actual facts about the app. Moreover, they had a more positive sentiment toward the app. Yet, overall the effect sizes of the statistical tests are rather small. This suggests a difference in

certain relevant aspects but not enough that we could describe the users overall as better informed.

RQ2: Do mental models of data collection and processing differ between citizens with high privacy concerns and those with low privacy concerns?

Privacy concerns were a focus on the initial public discussion about the CWA. Privacy concerns as a term is used when talking about a feeling someone can have toward the app, but it also refers to a person's general sentiment [77]. Utz et al. [208] found that the latter, the general sentiment measure by the IUIPC-8 (Collection), has a negative impact on the intent to install a CTA. Therefore, we were interested in whether we could relate these sentiments to assumptions. We report the results in this section. As for RQ1, we only report differences that were statistically significant ($p < .05$).

Collected Data and Technology For the data collected and technology used, the data paint an inconsistent picture: significantly more participants with high privacy concerns think that their distance from others (Awareness and Control, Q9d), the duration of contact with others (Awareness and Control, Q9h), their infection status (Awareness, Control, Collection, Q9i), the time of contact (Awareness, Control, Collection, Q9j), their location (Awareness, Control, Q9a), as well as information about how they use the app (Collection, Q9c) is collected. Yet, significantly more participants with low Awareness privacy concerns think that information about their phone model is captured (Q9f).

Regarding the technology that is used to capture encounters, participants with high Awareness and Control privacy concerns tended to agree significantly more frequently to the correct answer option, i.e., Bluetooth (S1).

Anonymity and Data Use Significantly more participants scoring low on Awareness privacy concerns and Control privacy concerns thought that it would be possible to assign their identity to their infection status (S3) compared to those with high privacy concerns. Our analyses could not replicate the effect we saw for the infection status for encounter data (S4). Counter-intuitively, participants with high Awareness and Control privacy concerns tend to think it less likely that their data are used to create advertising profiles (S7) and monitor their location (S8), while all participants with high privacy concerns (Awareness, Control, Collection) indicated significantly more often that their data would only be used for warning purposes (S5) or to monitor the infection incidence (S6).

Data Transmission and Storage Participants with high Collection privacy concerns, who generally tend to assume correctly what data is gathered, are more likely to assume that their data will be transferred to the cloud or a server for storage (S9). On the other hand, participants with high Control privacy concerns

tend to think that the encounter data and infection status are transferred directly between the users' smartphones (S10).

Data Access The assumption that the government has access to the user's location via the CWA is substantially more frequent among participants with low privacy concerns (Awareness, Control, Q10b). Further, participants with low values for privacy concerns (Awareness and Control) notably thought that the government had access to their encounter data (Q15b) and infection status (Q20b) more often.

Participants with higher Collection concerns were more likely than those with few concerns to think that companies involved in the development or operation of the CWA had access to their location data (Q10a).

In line with believing that involved companies can access the app's data, participants with high Collection concerns also think that hackers would have access to their data (demographic data, Q10e).

The government-affiliated RKI and public health departments are also more likely to have data access in the view of participants with high privacy concerns. These participants are more likely to think that the health department can access their demographic data (Awareness, Control, Q11 d) and the RKI can access their encounter data (Q15c) and infection status (Awareness, Q20c).

Warnings about encounters with infected people Individuals with high Awareness and Control privacy concerns are more likely to assume that warnings happen after a delay (16), while participants with low concerns believe that warnings happen directly or that infected individuals are shown on a map (S15). Participants with high scores on all three privacy concerns' scales also think that warnings are automatically issued when a positive test result is entered into the app (S17).

Perception of the app The data paints an ambiguous picture: high Collection concerns lead to greater risk perception (S19) and high Awareness concerns and high Control concerns lead to greater trust in official CWA information (S23). On the other hand, low Awareness concerns are connected with higher benevolence scores (S20).

Open Access and Importance of Data Protection Unsurprisingly, participants scoring high on all three scales of the IUIPC were significantly more likely to say that privacy played an important role for them in deciding whether or not to use the app (S25) than participants scoring low. We could not detect any difference for the knowledge (S26) or sentiments (S27) about the source.

Summary Testing for differences that would link the IUIPC-8 score to specific assumptions about a CTA did not result in a clear conclusion. However, we

were able to detect differences between the high and low scoring participants in different aspects. But again, for most fact-based scales, the differences are minimal.

2.4.4 Discussion

We surveyed 151 users, 151 non-users, and 50 past-users about the CWA. In our study, we found that most participants, users, non-users and past-users, hold misconceptions about data collection and processing in the CWA. These misconceptions include the assumption that users' location data would be captured, that data storage and processing are centralized, and that multiple parties, such as public health departments, would have access to the collected data. These findings were expected based on previous research. We were particularly interested in exploring whether we would find relevant differences based on the app usage or general privacy concerns (measured by the IUIPC-8 scale). In this section, we discuss the implications of our findings for developers, researchers, and policymakers.

Knowledge About App and Usage (RQ1)

We discovered that users seem to be better informed about data collection and processing in the CWA than non-users, while past-users are equally as well-informed as users. However, in absolute terms, the knowledge differences between users/past users and non-users seem to be rather small, as the effect sizes can mostly be classified as small to medium, according to Cohen [38]. Based on the many misconceptions of non-users, we expected bigger effect sizes. Hence, it might not be very useful to launch additional campaigns that aim to foster understanding of the CWA's technical functionality in an attempt to increase app usage. Instead, it might be more effective to focus campaigns on its usefulness rather than educating users on the technical implementation of data protection. Usefulness has been identified as a driver for the intention to use a CTA [213].

Can we talk about informed consent? The CWA is a complex technical tool that employs a fairly new approach to trace whether people have been in contact with each other. There is no metaphor based on in-person contact tracing that is already established in common knowledge and can be utilized to explain digital contact tracing. Previous, e.g., manual, approaches are based on the knowledge of who met whom or at least the person's location. Consequently, we believe it is not straightforward to explain decentral contact tracing as done by the CWA.

Even though a lot of effort was put into such explanations (e.g., with an explanatory film by the German government [91]), we see that even users show various misconceptions about the collection and processing of their data. We, therefore, cannot assume that all users have the necessary knowledge to consider them *informed*.

Insufficient information to provide informed consent regarding the actions of an app may serves as additional evidence that the privacy-as-control principle may not always fulfill its intended purpose in practice. This aligns with previous research in as online tracking [138, 92, 121, 153, 120, 73]. Therefore, it might be more purposeful to consider following the privacy-as-confidentiality approach more often. For some cases, making it a legal requirement, would ensure that data protection is guaranteed even in cases that are not a good example of a privacy-respecting app, as seen in the case of the CWA.

Why are users (slightly) better informed than non-users? Even though not perfect, users had a better understanding of data collection and processing than non-users. We see two possible explanations for this slightly better understanding: either users were already more aware of the technical functioning before they installed the app, or the post-installation usage experience leads to more accurate mental models. As we did not design our questions in a way that would allow participants to answer this, future work should investigate why users possess a better understanding of the app. This is important as many misconceptions are an overestimation of what data is gathered and who can access it. Though thinking the app did more than it actually did did obviously not prevent users from installing it, the non-users may have been deterred by that.

Detector of infected persons Previous research [202, 223] revealed that participants assume it is possible to get a direct and in-time warning if an infected person is close to oneself or see a map where infected users are located. Yet, when opening the app, it should become clear that this is not the case: no map is included in the app, and the only feature that might come close to a map was added on the app's dashboard as an overview of infection numbers in regions a user could like to be informed about. Notably, no region was presented on a map.

We sought to understand if the data from previous studies was due to misunderstandings or if participants actually thought so. Thus, we took extra care when designing the questions to exclude the aforementioned feature of getting an overview of the infection numbers. Since both these questions highly correlate, we assigned them to a scale, using the factor and reliability analysis as a basis (see Section 2.4.2). It is apparent that users (vs. non-users) marked these questions to be true less frequently (15% vs. 26,5%). It remains unclear why so many participants, even users, had this incorrect assumption and what the effect of this assumption on the installation status was.

The Role of Privacy (RQ2)

In this section, we first focus on general privacy concerns as personal attitudes and then on specific privacy concerns related to the use of the CWA.

General Privacy Concerns We found that participants scoring high on the privacy concerns' (IUIPC-8) Awareness and Control scales had a more accurate understanding of data collection and processing in the CWA than participants who scored low on these scales (RQ2). Awareness and Control are about proactive behavior, i.e., by definition, users scoring high on these scales are more involved in the handling of their data, we could see that resulting in a better understanding of the technology. The fact that the different scales represent different aspects and may also contradict each other (we cannot draw the same conclusion for Collection) is in line with the findings of Groß [93], who showed that the IUIPC-8 does not measure an overall privacy concerns factor and that the three scales should thus not be combined into one single value.

Specific Privacy Concerns In related work, participants expressed privacy concerns regarding the CWA itself [127, 148]. Yet, from these studies, it is unclear a) what people see as an issue and b) whether their assumptions match reality and, therefore, whether privacy concerns were based on that. With our study, we can shed light on the second point. Figure 2.12 shows that participants indeed had assumptions that would lead to less privacy than what is possible with the app (e.g., 71% assumed the app would access the user's location). Even though we cannot know for sure how participants evaluated a feature, several of them could be seen as privacy-invasive. Interestingly, several features (tracking the user's location, utilizing the user's identity, and adopting a centralized model) were explicitly not included in the app. So, this knowledge did not fully reach the population.

Despite this, several participants decided to install the app, even when assuming features that could be a threat to their privacy. Participants that installed the CWA overestimating data they have to share is maybe not ideal, as the CWA specifically foregone certain functions, but in the context of the application not per se a problematic situation.

Implications

At the time of writing this paper, the WHO had ended the global emergency status for COVID-19 [171] and the CWA subsequently went into hibernation mode [79]. Hence, while our work cannot contribute to developing a better app, we believe our work still addresses important aspects with regard to the informed consent debate and, maybe even more generally, people getting acquainted with novel technologies. Our results implicate that although extensive campaigns were launched to explain the CWA's technical functioning, users of the CWA were not able, since not being knowledgeable enough, to give their *informed* consent to the collection and processing of their data. Most understood what the app wanted to achieve, but not how. In the case of the CWA, presumably, no damage was caused as less data was collected and used than anticipated. At the same time, some participants overestimated the app's capabilities

and maybe even installed it, or refrained to do so because of their assumptions. The CWA, is a special case as a privacy-by-design approach was taken to the development due to the broad social debate and government involvement. The CWA may also be a special case in that the goal was to get as many people as possible to install it, and it had no commercial interests that may have conflicted with the will to be transparent about the data usage. However, other software is often developed exclusively by commercial companies with a financial interest in their users' data without any accompanying public discourse. If we apply our results (that a relevant portion of the participants over and underestimated the app's functionality) this could result in users giving unintended consent to data collection and processing due to a lack of understanding. Thus, we argue that this study presents evidence that we need to find new methods for dealing with such cases, e.g., by making privacy conscious designs more often a legal requirement. Still, for some applications, it may be necessary to collect a wide range of personal data to provide the intended functionality, and the strictness of the legal regulations must be weighed against the app developers' scope of action. Hence, as an alternative and less stringent solution, trusted observers could provide meaningful ratings.

Our results also hold implications for policymakers, service providers, and researchers from the usable privacy and security area.

In the usable security and privacy (S&P) research community, we sometimes experience an implicit assumption that users would behave "better" (more secure, more privacy-conscious) if only they had a better understanding of technology. Accordingly, efforts are often made to enable that by improving awareness and understanding of technologies that improve security (such as End-to-end encryption (E2EE)) or data collection practices in the hope that this will lead users to act with their security or privacy in mind [97]. For example, researchers aim to identify explanations or metaphors that can make the principle of E2EE and differential privacy tangible for lay users [175, 119]. If we apply this principle to the CWA, we might assume that more people will look positively on the app, maybe even use it, if they understand that the app does not pose a threat to their privacy due to its sophisticated technical functionality. Yet, our results indicate that the decision for or against using the CWA is based more on trust in the app than influenced by how well one understands the technical principle behind it. Based on this, targeting a "better" S&P behavior via improving awareness and understanding is not the optimal way (but we still think it is necessary!). Establishing data protection by design legally or through mandatory use, e.g., of E2EE in the corporate context, may prove to be more promising in the short term.

2.4.5 Conclusion

We conducted a survey study to understand users' and non-users' understandings of the German COVID-19 CTA, the CWA. We additionally shed light on

whether general privacy concerns measured by the IUIPC-8 also relate to assumptions about data collection and processing within the CWA. Generally, we saw that many participants had misconceptions about the functionality of the app. We tested participants' differences in their understanding of the app, finding that users were significantly better informed in several areas. However, even users exhibited several incorrect assumptions about the CWA.

2.4.6 Acknowledgments

This research work has been co-funded by the Deutsche Forschungsgemeinschaft (DFG, German Research Foundation) – 251805230/GRK 2050, and by the German Federal Ministry of Education and Research and the Hessen State Ministry for Higher Education, Research, Science and the Arts within their joint support of the National Research Center for Applied Cybersecurity ATHENE. We thank the Werner Siemens-Stiftung (WSS) for their generous support of this project.

Chapter 3

Social Authentication - Can Johnny be a whistleblower

The previous chapter focused on whether the participants decided to install an app, the Corona-Warn-App (CWA), and why. I found that participants did not always understand the CWA. This chapter is about a protocol called Social Authentication Protocol (SOAP), which was explicitly developed in the hope that it would be understood and, therefore, usable. SOAP is a protocol for authentication ceremonies, i.e., sharing public key material, developed by colleagues of the "Centre for Cyber Trust" project of the Werner Siemens-Stiftung. Part of the public and scientific debate about Contact Tracing App (CTA)s was that mission creep and public surveillance should be prevented. SOAP is a protocol that offers the possibility to recognize and protect against this in the field of instant messaging. This chapter presents two lab studies on the Signal App [181] in combination with SOAP [134] that I conducted to test whether SOAP would fulfill its goal.

Disclaimer: The contents of this chapter are based on the published paper " Can Johnny be a whistleblower? A qualitative user study of a social authentication Signal extension in an adversarial scenario " presented at the twentieth Symposium On Usable Privacy and Security (SOUPS) in 2024 [102]. This was joined work together with with my co-authors Julia Angelika Grohs, Christian Tiefenau, Eva Gerlitz, and Matthew Smith. As this work was conducted with my co-authors as a team, this chapter will also use the academic "we" to mirror this fact. I designed the study with the supervision of Matthew Smith and the help of Christian Tiefenau and Eva Gerlitz. The code was written by Christian Tiefenau and me. I conducted the lab studies with the help of Christian Tiefenau, Eva Gerlitz, and Julia Angelika Grohs. I analyzed the data. Before compiling the paper for publication, Christian Tiefenau, Eva Gerlitz, Julia Angelika Grohs, Matthew Smith, and I jointly discussed the study's implications.

3.1 Introduction

SOAP [134] is a protocol for authentication ceremonies in the context of End-to-end encryption (E2EE). E2EE is a well-known and broadly applied technology in messaging apps. Its implementation helps to improve the privacy of billions

of people. However, E2EE cannot provide authenticity without the interaction of the users. To have authenticity, communication partners must ensure that the correct key material is used, i.e., the service provider is not tampering with the keys to mount a person-in-the-middle (PITM) attack. The task of comparing the key material of the communication partners, e.g., by meeting in person and showing them, is called an *AC*. By correctly carrying out an authentication ceremony (AC), users can be sure they are talking confidentially with the right person. However, the default in current messaging apps is to trust the first keys given to users by the provider without encouraging an AC [7] and inform users when these keys change. Studies show that few users run authentication ceremonies, and many users do not know the cryptographic notion of authentication and how to handle the corresponding ceremonies [105, 59]. In our assessment, a reason why few users have a reason to verify keys is that even without verification E2EE provides a good level of protection as mass surveillance is resource-hungry and disincentivized for the attacker; getting caught is fairly likely due to key-change notifications that can be noticed by the provider or experts, e.g., facilitated by key transparency [144, 130, 228]. However, targeted surveillance can still be a threat since it is technologically possible, and the risk-benefit ratio for the attacker could be worthwhile. Consequently, we believe that if there is a need for authentication ceremonies, it is most pressing in high-risk scenarios, e.g., when one is a political dissident, a whistleblower, or a government employee. While the single tasks that are necessary for authentication ceremonies can be done quickly and with rather low false-acceptance rates [212, 180], studies provide evidence and researchers argue that current authentication ceremonies are difficult and error prone [176, 106, 225, 105]. A fairly new solution for remote[1] authentication, *social authentication (SA)* was suggested by prior research and leverages social networking sites as a trust anchor [134, 210, 123].

The idea behind this solution is to reduce the verification task to something users can already do and intuitively grasp. For SA, users do not need to compare key material directly; instead, they must decide which identity provider, e.g., a social media site, to trust and recognize an already known account. As such, users need to have knowledge about the contact they want to authenticate and know their identifier (e.g., Alice42) on the chosen identity provider (e.g., facebook.com). Vaziripour et al. [210] tested the concept in a laboratory study and reported that participants found the concept convenient and matched "how participants thought of verification." Vaziripour et al. found the approach to have good usability. However, their solution was tested under ideal conditions, i.e., without any attackers. Nevertheless, the researchers noted that SA makes identity spoofing and impersonation attacks possible. Currently, no work on SA in an attack scenario exists. To fill this knowledge gap, we conducted two user

[1] "Remote" refers to a setting where the two communication partners carry out an AC without meeting in person. Although we phrase authentication ceremonies as a task for two users, most of the time, it works similarly for more than two.

lab studies where we simulated an attack scenario and compared SA to the already established authentication ceremonies of key fingerprint comparison and QR codes.

This work contributes the following:
An expansion of the existing literature on authentication ceremonies by testing an attack scenario in a **user study** of a SA approach. This study is the first to offer insights into **social authentication in an attack scenario**. We were especially interested in the participants' reactions toward impersonation attacks, i.e., how often they would notice the attack and how they would proceed with a given task.

We created a scenario that resembles, more closely than previous work, a realistic use case for users needing an authentication method. To motivate the participants to authenticate and mimic real-world situations, they had to act as whistleblowers in an authoritarian regime and contact journalists. This **study design with a scenario with reasonable participant motivation** allowed us to observe the entire process of the authentication ceremonies. In contrast to Vaziripour et al.'s study [210], which proposed a form of SA, Linker et al. [134] formally defined SA and presented a protocol with proven security properties. They also developed a prototype that worked, with limitations, within the current internet eco-system. This means our results can be directly applied to their prototype and hopefully increase the security of users in high risk scenarios.

During our analysis, we were guided by the following research questions:

- **RQ1 - Detection**: How resistant is SOAP to impersonation attacks?
- **RQ2 - Reaction**: How do participants react to a detected impersonation attack?
- **RQ3 - Perception**: What are users' perceptions of SOAP (usability, trustworthiness), with a focus on the identity providers?

The rest of this section is structured as follows: In Section 3.2, we provide a short overview of relevant authentication methods, their shortcomings, and the concept of SA. In Sections 3.3 and 3.4, we present the user studies, and in Section 3.5, we discuss implications and further directions for research and messaging app developers.

3.2 Context and Related Work

In this section, we summarize authentication ceremonies in the messaging app domain and related work about them to put social authentication into context.

Authentication Ceremonies

Comparing key material, a process called an AC has scarcely changed in the last few years. Via an AC, a PITM attack can be detected, e.g., if the attacker uses a key substitution attack [106].

Material for comparison is always based on the public key, but the visualization differs among apps [106, 7]: Signal, using a visualization that was very close to the technical reality, initially displayed two fingerprints before changing to concatenation and currently displaying a single safety number [146]. In addition to that, Signal also offers a QR code, which is a different representation of the single safety number. A recent version of Telegram (iOS 10.3.1) shows a scannable identicon, similar to a QR code, and a hex notation "generated from hashes of the DH secret chat keys" [201]. During phone calls, smileys are shown [199].

The success of an AC has its challenges. Herzberg et al. [106] structured these as deciding that a ceremony is needed, finding the ceremony in the user interface, executing the ceremony, understanding the result, and acting on it.

As it is assumed and evidenced [176, 211] that users struggle with authentication ceremonies, studies looked at each of the steps in the whole process and tried to improve them. Vaziripour et al. [212] worked on guiding users to the ceremony interface. With opinionated design, they were able to lead 90% of their study participants to the ceremony. Wu et al. [225] worked on users' comprehension of safety number change notifications and found a need to communicate the possible risk to users as a motivation and basis to decide. Shirvanian et al. [180] studied whether the comparison act itself could be a problem. They found evidence that in a remote setting (i.e., when users do not sit next to each other), comparison can be an error-prone task, mainly because users need to compare codes between two apps on the same device, with the need to remember the code. Tan et al. [198] and Livsey et al. [135] researched how different visualizations impact the comparison act. Although Livsey et al. found that their participants did not make many mistakes, Tan et al. found that visualization can greatly impact the outcome in an attack scenario, with success rates for the attacker varying between 6% and 72%. All these studies and the methods used rely on the same AC principle: a direct manual exchange and comparison of key material to authenticate the communication partner. As described in the next section, social authentication relies on a different principle.

Social Authentication

In the literature, two different topics are referred to as social authentication. According to Jain et al. [114], SA describes when Alice wants to log in to a service and another user, Bob, who is connected to Alice on the (social media) platform, is asked whether they are allowed to. This can be triggered, e.g., as a step in a risk-based authentication scheme. However, Vaziripour et al. [210] described

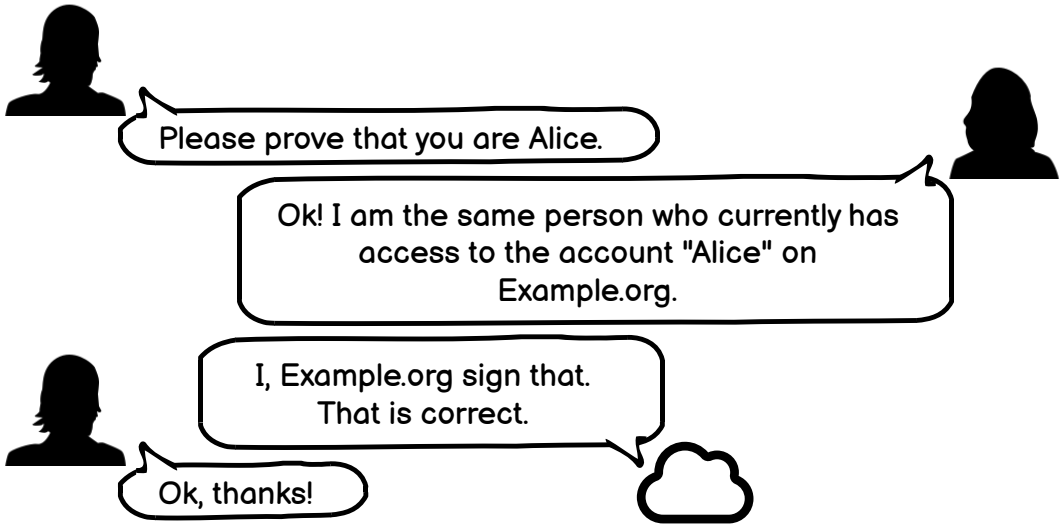


FIGURE 3.1: The communication flow of social authentication, where Alice proves her identity by accessing Alice@Example.org, enables the receiver to verify the sender's identity.

SA as an AC completed through "social media." In SA, public key material is distributed and compared through a social media provider. In this paper, we refer to this second notion of SA as an AC. The basic idea of this AC is to shift the challenge of the ceremony itself from selecting a secure channel, exchanging the key material, and comparing the fingerprints to a different task: deciding what provider to trust and recognizing an identity.

An early application where this notion of SA is in place is Keybase. On Keybase, a user can provide proof of having access to an account by posting material on it. Afterward, other Keybase users can decide whether proof of access to that account is enough for them to identify the person [123]. Vaziripour et al.'s [210] proposed system is very similar. The researchers envisioned that Signal users would log in to their social media accounts during configuration and the public key material would be posted there. Similar to the scheme utilized by Keybase, this would allow observers to see the material. For example, if Alice wants to check whether the E2EE on Signal is PITM-free and authentic, they could check whether Bob has provided a reference account on a trusted social media platform, in the following called identity provider (IdP). As the key material is posted online, it can be compared automatically and asynchronously. The decision Alice has to make is whether they trust the IdP and whether the account provided by Bob belongs to the person they want to contact. Vaziripour et al. [210] tested their idea in a lab study (21 participant pairs) and an online survey (N=421). They let the participants communicate via Signal and, if not initiated by themselves, guided them to the AC. Here, the participants were able

to choose between three verification methods: *social media* (social authentication), *in person*, and *phone call*. The participants were allowed to choose from all three methods and were asked to use the remaining two after selecting one. The researchers found that the *social media* verification method had the best Single-Ease-Question (SEQ) score but was less trusted than the *in person* and *phone call* methods. Additionally, the participants chose the *in person* method first (n=20) more often than the *social media* method (n=12). The average configuration time of the *social media* method was 2 minutes and 32 seconds. On average, verification (which, in this case, meant looking at profile names and pictures) took 34 seconds. Varziripour et al. concluded that social media was not perceived as a highly trustworthy provider of authentication, but the participants liked the asynchronicity, that it worked remotely, and that it was partially automated. As the challenge of the AC changes, so does the attack surface. The participants in Varziripour et al.'s study mentioned the attack vector of fake profiles, which indeed seems to be a major challenge for SA. Additionally, the key material has to be public. This could be problematic for some users due to privacy considerations. Another recent proposal, "SOAP" [134], mitigates this and aims to find a way to bootstrap SA in the current internet without too much effort from the provider's site. Hence, SOAP utilizes IdPs, not necessarily social media providers. An IdP could be any entity providing an OpenID Connect service, hoping for a relatively fast and easy adoption. If Alice wants to check the security of the chat with Bob, Alice asks Bob to prove that they have control over an account at a specific (listed) IdP. Bob uses their fingerprint (salted and hashed) in a request. An IdP signs the requests, and Alice now has a statement from the IdP that says: With whom you are talking to, identified by the fingerprint, has control over account "XYZ" on my platform. A simplified visualization of the conversation flow of SOAP can be seen in Figure 3.1. To the best of our knowledge, currently, no research on SA attack scenarios exists. This gap is filled with the studies presented in the remainder of this chapter.

3.3 User Study 1 - Simple User Interface

We tested SOAP in two lab studies, and in this section, we describe the first of the two user studies conducted. We implemented a simple SOAP [134] interface for the Android Signal app to see how people interact with it and whether attacks would be detected.

3.3.1 Methodology

We conducted a lab study where we tested the detection rate of and the reactions to an impersonation attack on a new AC. The study documents, original and translated, can be found in the Appendix D.1.

Setting and Scenario

When developing our scenario, we looked at previous studies on authentication ceremonies. Herzberg at al. [105] reported that participants recognized to act differently depending on the situation, e.g., based on the importance of a contact, and Wu et al. [225] discussed participants' need to be able to assess the need for an AC. Previous studies observing human behavior and authentication ceremonies used very simple scenarios [180] or settings where there was little explicit (intrinsic or extrinsic) motivation for the participants to behave securely [212, 210, 211, 225, 176, 105]. We wanted our participants to be motivated to conduct the AC, so we provided a scenario that gave them a reason to do so: a whistleblower scenario. We hoped the participants would understand the importance of being cautious, as they know the consequences of deanonymization, e.g., losing their job and reputation, prison, or even death. To check the realism of our scenario, we searched news sites and found examples where Signal was proposed as a channel for communication [4, 156, 133, 203, 232, 162].

In some previous studies with authentication ceremonies, participants were invited in pairs [211, 176]. Some of the participants knew each other [211]; hence, they would have been able to judge whether the contacted person was the correct individual based on voice, looks, and behavior or meeting in person. We reduced these mitigating strategies through the scenario so the participants could not know the person they interacted with and could not verify the person via human characteristics.

Taking all this into consideration, we ended up with the following scenario outline: The participant, named Alex, is a whistleblower. They have a colleague and friend named Hannah, who sent them documents revealing a political scandal via Signal. Their conversation was verified in person before the receipt of a .zip file with crafted sensitive data. Hannah is not on site and is only reachable via Signal. Alex's task is to contact three investigative journalists and send them the documents after ensuring they are interested in the data and the communication is safe. Alex receives information about these journalists on business cards (see Appendix D.1 for details). As part of the introduction, the participants were told that the business cards came from a trusted source. Communication could only happen via Signal; other channels were not allowed. Each journalist had one intended possibility to be verified, which we printed on each business card: **Amira via safety number**, **Michael via QR code**, and **Anne via SOAP**. This way, the participants were nudged to use every method at least once. However, the participants were unaware that the authoritarian government of the scenario was suspicious of Alex and all connection attempts were attacked with impersonation attacks. So, all the verification checks failed: the safety number shown in Signal differed from the number and the QR code on the business card, and for each SOAP request, the provider or identity did not match. This put Alex in a no-win situation. The only correct behavior for participants was to abort all communication attempts. This was explicitly allowed in the task description.

We opted for this extreme scenario because it is realistic, and authentication ceremonies need to be able to protect their users from it.

Recruitment and Compensation

The study participants were recruited from a usable security lecture in an undergraduate program. For their participation in the study, the participants received bonus points for the lecture's exam. In addition to the points, the participants were told they could get a bonus cash reward of up to €20. The participants started with €5, and if they securely transmitted the sensitive data from Hannah to a journalist, they received an additional €5. They lost everything if they got caught, e.g., by sending the data to the wrong person. We provided this reward to motivate the participants to contact as many journalists as possible and try the different authentication methods while behaving securely: the participants needed to weigh the risk of not sending the data and, therefore, receiving less money versus sending the data and risking losing everything. We hoped that this would lead them to act cautiously and align their interests with the scenario. The participants started the study with €5 so that they had something to lose from the beginning on. We told them we would share their results with them at the end of their study session. To eliminate any motivation to collaborate with fellow students, we paid each participant €20 and asked them to keep the study details confidential. The study took place in July 2023.

Ethics

We received IRB clearance for the study and adhered to the German data protection laws and the GDPR in the EU. All participants consented to their participation and the use of the data for research purposes before participating. The participants were informed that they could terminate their participation at any time without negative consequences and that, in such a case, all the respective data collected up to that point would be deleted. The participants received bonus points for the lecture exam, which could also be obtained in other ways. Also, the participants were told they would receive bonus cash rewards for successfully transmitting data. As all journalists suffered an impersonation attack in this study, no participant could receive any bonus beyond the basic €5. We paid €20 to each participant and informed them about this in the debriefing.

Study Protocol

The study was conducted in three parts, as described in the following.

Part 1 - Intro The participants read and signed the consent form. Afterward, they received the material and were instructed to read the scenario text. Each participant was handed a pen, paper, and a smartphone with Android 13 and

our modified version of Signal installed. Additionally, we handed them the three journalists' business cards (see Appendix D.1) in random order to counter ordering effects. The journalists each had an existing phone number to enable Signal communication. Further details on the business cards were fictive to avoid selection bias based on a newspaper's familiarity or reputation.

Part 2 - Scenario We asked the participants to think aloud while working on the task, audio recorded the whole procedure, and screen recorded the smartphone. Their task was to choose journalists and try to contact them securely. The researcher giving the briefing was present in the room during these steps and ended the scenario after about 30 minutes to keep the whole study under one hour. The researcher had the option to extend the time a few more minutes if a participant was in the final stage of sending or verifying. A second researcher who was not present in the room manned the journalists' Signal accounts. They had a playbook (see Appendix D.1) that was expanded in new situations. If a participant asked for a communication method other than Signal, this was denied, as is the case in real-world scenarios. The responses to the SOAP requests were randomly selected from three cases:

- Wrong provider - correct identifier
- Correct provider - wrong identifier
- Currently no access available

If multiple IdPs were asked for in a single request, the cases were picked without duplicates, so that with three asked IdPs, there were three different cases.

Part 3 - Outro When a participant told the researcher they were done or the study time was up, they needed to complete a survey (see Appendix D.1). After this, there was a short interview followed by a debriefing.

Analysis

We used qualitative and quantitative data to capture the results. As per our research questions, we were interested in the following:

1. Who would try to authenticate via a ceremony? As we added the red bar [212], we assumed this would be everyone.
2. Which provider would be chosen on SOAP? We assumed that most of the identifiers on the cards would be used.
3. Would the participants detect the attack via SOAP? We assumed that most of them would.

4. How would the participants react? We assumed that the participants who detected a failed ceremony would abort contact.

5. How many participants would fail the task? From the overall tone in related work, we assumed a few would.

Pilot Study and Participants

We conducted four pilot studies, recruiting participants from our research group's contacts. For the study, we recruited 13 participants from an undergraduate usable security and privacy lecture. We excluded the data of three participants due to UI bugs and another participant who stated that they knew beforehand what the study was about. Thus, we were left with data from nine participants that we analyzed (Table 3.1). We did not collect much demographic data as we assumed that the few participants would be identifiable from their data, and we had no demographic-specific hypotheses.

3.3.2 Technical Implementation

Linker et al. [134] presented an accompanying prototype that implements the technical protocol but does not hint at its capabilities to the user. Only one button in the app's share menu suggested the usage of SA. So, the verifier has to know that SOAP exists and somehow agree with the to-be-verified person what identities and IdPs are available and then ask for proof. For this study, we were not interested in whether people could find the icon, and we did not want to explain the idea in a workshop. Seeing that the prototype's design was not ready for our purposes, we adapted it to the needs of our study. We used the Signal app because the prototype builds on it, it is open source, and previous studies also used Signal. In the following sections, we detail relevant elements of the technical implementation.

Hint to the Ceremonies

To test SA, we were interested in pointing the participants directly to the relevant parts of the interface. Vaziripour et al. [212] successfully led users to the authentication ceremonies with a clear, visible red bar above the text entry field, and we adopted the same method. A click on the bar triggered a dialog with the three ceremonies (see Figure D.3c in Appendix): QR-Code, Safety Number, and SOAP.

QR Code and Safety Number

When the participants clicked on the QR code or safety number button, they landed on the same, slightly modified safety number page in the chat settings as in recent versions of Signal. There, a QR code could be scanned, and the safety

number read. A message must have been exchanged with the contact for a chat to have a safety number. If the participants tried to access this page without prior communication, a popup reminded them that a first exchange must happen. Please note that although Signal provides a unique safety number per chat, it is only a concatenation of two per-user numbers. So, just the half belonging to the contact had to be checked. Because of this, we could write Amira's number on the business card and added an explanation of this to Signal's settings page.

SOAP - The Social Authentication Proposal

Choosing SOAP opened a window that asked the user to select an IdP and what accounts the chat partner should prove access to (see Figure D.1a). The user could choose as many of the given IdPs as they wanted and optionally fill in their communication partner's expected account names on these platforms. Although the original SOAP protocol [134] currently does not support requests for an arbitrary provider, we added an option for it. After clicking "Next," the request message was pre-filled in the chat window and could be sent to the chat partner. Currently, very few providers can actually be used for SOAP, and the original prototype only supported Microsoft and Gitlab. As we wanted more providers, we omitted the technical procedure and the journalists just responded with a predefined formatted string interpreted by Signal as a valid response on the participants' side. After receiving the response (Figure D.1b), users could mark the user as verified. Besides the additional providers and the simplifications to mimic PITM attacks, SOAP and our interface can be directly used to add SA to Signal.

3.3.3 Results

In this section, we describe the results of our lab study. First, we describe the general usage of the ceremonies and how successful our attacker was, and then, we list the themes related to failures.

Used Methods and Outcome The UI adaption and the scenario text seemed to work, as all participants except CS-7 started every AC at least once. In general, the QR code from Michael's business cards was checked correctly. The safety number was used not only with Amira but also with the other journalists: the participants asked for the safety number, and the journalist sent them the current one via chat.

Even though we intended for each journalist to be authenticated with exactly one method (safety number, QR code, or SOAP), all the business cards were provided with at least an email address. Following this, SOAP was not only used for Anne but for other journalists as well, with the work email being the most frequently used IdP (see Table 3.2).

ID	Sent to			ATI[70]	Reason for Failure
	Anne	Amira	Michael		
CS-1	○	○	○	3.9	
CS-2	○	●	○	6.0	Typosquatting
CS-3	○	●	●	5.6	Typosquatting
CS-4	○	○	○	5.8	
CS-5	○	○	○	5.3	
CS-6	●	●	○	4.4	Typosquatting
CS-7	●	●	●	2.9	"Marking" makes it secure
CS-8	○	○	○	2.9	
CS-9	○	○	○	4.4	

TABLE 3.1: Overview of the participants' results. Four sent data to at least one journalist (marked by ●). The "Reason for Failure" column matches a theme in Section 3.3.3.

Provider	**# of requests**
Work email	9
Twitter	8
LinkedIn	8
Instagram	8
Facebook	7
Gmail	4
Reddit	3
Telekom	2
Pinterest	2
iCloud	2

TABLE 3.2: Frequency of how often each IdP was requested in the first study. The work email is the provider most frequently requested, and in the current protocol proposal, it is not included.

Overall, four of the nine participants forwarded the data to at least one journalist.

Ways to Fail

The participants tried different methods to mitigate the paths they attempted that did not work. All but one failure in the scenario can be traced back to SOAP. Specifically, we identified three reasons for failure.

Typosquatting: Three participants did not notice the typosquatting attack in SOAP or assumed it to be all right, e.g., CS-3 recognized a mismatch of the requested provider but decided that one can only verify a ".de" identifier if one has access to it. They all correctly saw that the safety number and QR code were invalid. We assume that a more sophisticated attacker could have fooled more users.

"Marking" makes it secure: CS-7 contacted every journalist with a cover story. Afterward, they clicked on the safety number site, marked the journalists as verified, and sent the data. While that initially seemed rather strange to us, CS-7 explained in the interview and survey that they expected the chat to be verified and encrypted after this action. CS-7 saw the SOAP request screen but closed it as they thought it was unsafe. CS-7 was also aware of the possibility of a QR code scan but decided not to use it as they feared surveillance through their phone camera.

Trust Chaining: Additionally, two of the participants verified one journalist and asked this journalist for the safety number of another journalist. The attacker was able to provide the number seen by participants. With this, the participants even accepted journalists who were previously perceived as suspicious.

Scenario

We noticed topics related to our scenario that influenced the participants' behavior and, therefore, the handling of the authentication ceremonies. For all the methods, it was necessary to contact the journalist via a possibly insecure channel before deciding whether that person was the correct individual. The participants questioned whether this first contact could already be seen as a crime and tried different mitigation strategies. Some utilized cover stories to mitigate this. While this was not intentional and a distraction, it shows that our participants bought into our scenario. Others thought activating disappearing messages would circumvent this. However, some participants had no problems with this at all and started with an already potentially revealing message such as "Hello, I have an important file for you that can change people's lives." Describing a scenario in a way that provided enough motivation without providing too many details proved difficult. A participant questioned what power the government has. Depending on its capabilities, SOAP might be rendered useless. We assume that conducting the study in a lab setting might have impacted the participants' behavior as they further communicated with the journalists even when the SOAP request failed, e.g., they noticed a failed request yet asked for a second or tried a different method to verify the person.

Concepts and Mental Models of Authentication Ceremonies

We noticed that the participants often lacked understanding of either authentication ceremonies in general, as expected, or the idea of SOAP. First, the concept of the IdP was unclear. For example, the participants thought that if a contact uses an email address as an account name (identifier), this contact must have access to the email address. Another misunderstanding bound to the interface was that the identifier is the provider, e.g., the participants inserted the email address in the provider field.

One issue we discovered was that several participants were not aware and did not seem to understand what consequences a safety number mismatch has or could have, even after consulting the official FAQs. While Amira's safety number was on her business card, the chat's safety number was double the length, as it is a concatenation of the safety numbers of both parties. Initially, this confused the participants, but reading the extended text below the number cleared things up.

Further Observations

The participants wanted to fall back to other methods that may be easier to attack in the future through deepfakes, e.g., asking for a photo or a call. The participants also used on-device techniques to react to an insecure chat, such as renaming contacts, deleting chats, or renaming contacts to "Unsafe [Name]." Another participant did not want to use the QR code due to fear of camera espionage. Repetition was a common reaction. The participants often scanned the QR code multiple times to ensure it was not a one-time problem.

3.4 User Study 2

After conducting the first study with SOAP and observing where mistakes could happen, we adapted the UI to prevent them. In this section, we describe the follow-up study where we wanted to test the changes. The main differences from the first study are as follows:

1. We adapted the SOAP interface to reduce possible attack surfaces.
2. We recruited a more general sample.
3. We added a new pre-registered SOAP information as a between-subject condition.

Details of the procedure and changes are provided in the following section.

3.4.1 SOAP Design/Technical Implementation

For the second study, we made several changes to how users interacted with the SOAP interface. We also tested a change in the SOAP protocol itself with half of the participants. The revised UI and the flow of the interaction can be seen in Appendices D.2 and D.3. Also, the source code is available at `https://osf.io/dsyfr`. The following modifications were made:
1. We added a link to start a SOAP request on the safety number site in the settings.

2. The red banner no longer disappeared after verifying the person. Instead, it turned green. This allowed a faster, more direct way to the setting page and a clear indication of the chat's status.
3. To reduce the attack surface for typo attacks and to match the current technical landscape, we removed the option to ask for a custom identity provider. We also reduced the number of providers that could be asked for. Because we had a fixed list of providers, we could simplify the detection of attacks. An unknown or unexpected provider directly led to a warning.
4. Based on the participants' comments and Vaziripour et al. [210], we assumed that a non-social media company would be favored and seen as more trustworthy. Therefore, we added Amnesty.org as a provider option.
5. We reworked the visuals of the UI, added more text, and added guidance to the interaction of the SOAP responses depending on the outcome, e.g., obstacles to send in the case of an incorrect response.
6. Because the participants in the first study were afraid of sending even a single message, they did not trigger the AC since this could only be started when communication was initiated. So, we wondered whether SOAP could be implemented without an interaction. To test the concept on the user site, we added a between-subject condition where we prepared a SOAP response for Anne without a prior request that appeared when opening a new chat (see Figure D.3b). Technically, this would be possible in the same way the provider's server shares the public keys or the material could be posted publicly as proposed by Vaziripour et al. [210].
7. We fixed some glitches in the UI.
8. To prepare for a more general, less tech-savvy sample, we rephrased "social authentication" as "proof of identity".

3.4.2 Methodology

We kept the scenario from the first study but modified the wording of the new UI based on the experience of the first study and with the expectation that the new sample was less tech-savvy.
1. We changed the phrasing of the scenario, e.g., the reader was addressed more formally.
2. We added additional demographic questions to the survey to learn more about the occupation of the participants and slightly reworded questions.
3. We added a quiz before the participants started the scenario (see Appendix D.1). The quiz consisted of seven questions about the scenario. The participants could answer the questions as often as necessary to get all the answers correct. We did this to ensure the relevant parts of the scenario were understood.
4. Half the participants were assigned to a new condition (pre-registered SOAP). We halved this group again by the provider/identity pair they would see: half of the group saw the identifier for Facebook on Amnesty (Anne_Baler on

Provider	Correct Identifier	Identifier available to the attacker
Amnesty.org	anne-baler-98746524b	anne-baler-13885412b
Facebook.com	Anne_Baler	AnneBaler
Gmail.com	n.a.	anne-baler@gmail.com
Twitter.com	@AnneBaler	@AneBaler
Amnesty.org	n.a.	a.patel@amnesty.com
Facebook.com	n.a.	Amira_Patel_86
Gmail.com	n.a.	patel_amira_86@gmail.com
Twitter.com	n.a.	@apatel
Amnesty.org	n.a.	m.kobel@amnesty.org
Facebook.com	n.a.	Anne_Baler
Gmail.com	n.a.	michael_kobel@gmail.com
Twitter.com	n.a.	@michael_kobel

TABLE 3.3: This table displays the identifier the attacker sent and what the correct one would have been. Providers without any correct identifier are marked as "n.a.". These instances occur when the participant could not determine the correct identifier. Participants received one of three responses: a) no identifier, simulating no current access to the account, b) an incorrect identifier for the requested provider, or c) a known identifier that is correct but for a provider different from the one requested.

Amnesty.org, condition "pre1"), and half saw a typo in the identifier (@AnneBaller on Twitter.com, condition "pre2"). We decided to do this to get as many different perceptions as possible. We assumed the participants would most likely recognize the typo but might make a slip with the line on the business card and accept the incorrect assignment of identifiers. The participants' assignment to the condition can be seen in Table 3.4.
5. When the scenario time was over, we asked the participants whether they wanted to make any further decisions.

SOAP Attackers Capabilities The first half of the participants had the same attacker as the first study. For the second half of the participants, we made the attacker stronger to adapt to the new UI. SOAP does not submit the identifiers the requester expects. So, the attacker does not know whether the requester filled in identifiers. In the first iteration of the interface, if a provider was requested and the response did not contain the provider, it was marked as a missing provider. The attacker could send an accompanying message like "Sorry, I currently have no access to this account," hoping the requester would not mind. In the more opinionated second iteration of the interface, any deviation from the request was marked as a failure. So, for the second half of the participants, we changed the attacker. The attacker would always send some form of identifier, hoping that the requester had not filled in an expected identifier. If no identifier was filled in during request, the participants had to decide whether the identity submitted was sufficient. The concrete list of available answers can be seen in Figure 3.3.

Recruitment and Participants

After multiple iterations of UI developments, we implemented countermeasures to address the problems we identified in the first user study. We recruited participants via a mailing list of a behavioral economics lab where studies can be distributed. To recruit 21 participants, an invitation was sent out to 3000[2] randomly picked mailing list receivers over 18 years old. The behavioral economics lab has a strict no-deception rule, so we had to change our reimbursement scheme. In the first study, we reminded the participants that if they got caught, they would lose all their bonus cash rewards, but we paid everybody in full, regardless of whether they made a mistake. To keep a certain amount of risk/reward in the payment scheme for motivation, we designed the following payment scheme for the second study. The participants received a base pay of € 15 and had the chance to receive an additional € 9 (€ 3 for the correct decision for each journalist). If they made a wrong decision, the entire bonus cash reward would be lost. We followed that scheme with one exception: P2 did not send any message and thus stayed safe, but P2 also did not interact with the system at all. To gather more information, we asked them to do so. While they later made a mistake, we paid out the bonus in full since their first behavior was safe.

We had a mix of participants who had used Signal before and new users. Eleven out of 18 participants did not use Signal before the study. Also, most of the participants (15) never checked the safety numbers of their contacts in any app. The ages ranged from 21 to 46 with a median of 24. One participant did not give their age. The study took place in October 2023.

Ethics

As in the first study, we received IRB clearance for the study and adhered to the German data protection laws and the GDPR in the EU.

3.4.3 Results

In general, seven out of 18 participants failed the task by sending the data to at least one journalist. Table 3.4 shows an overview of all the participants and to whom they sent the data. Most tried all the available methods. The UI improvements generally prevented the mistakes observed in the first study. Only one participant (P3) failed because of a mistake that can be attributed to SOAP. Nonetheless, the failure rate was still high, but in the following section, we describe in detail what we observed and why this is still a somewhat promising result for SA.

[2]We had no control over how many people were contacted.

Reasons for Failure

The instances where the software failed to protect the seven participants can be categorized into four categories: a) in-band safety number comparison (P8, P9, P10, P6), b) clicking too fast (P3), c) gambling for money (P13), and d) emotional stress (P2). The following provides more details on those themes.

ID	Study Cond.	Sent to			Anne's IdPs				Total Study length (m)	ATI	Tried method (Q6)			Reason to Fail
		Anne	Amira	Michael	A	F	G	T			SOAP	QR	Safety	
P1	pre1	○	○	○	○	○	○	○	42	3.9	●	●	●	-
P2*	ctrl	●	●	●	○	○	○	○	51	3.4		●	●	Stress
P3	pre2	●	○	○	○	○	○	○	36	2.3	●			Fast Clicking
P4	ctrl	○	○	○	●	●	○	●	44	5.1	●	●	●	-
P5	pre1	○	○	○	●	●	○	●	38	4.3	●	●	●	-
P6	ctrl	○	●	●	●	●	○	●	60	3.4	●	●	●	In-Band Exchange
P7	pre2	○	○	○	●	●	●	●	57	4.0	●	●	●	-
P8	ctrl	○	●	○	●	●	●	●	51	3.0	●	●	●	In-Band Exchange
P9	pre1	○	●	●	●	○	●	●	45	5.6	●	●	●	In-Band Exchange
P10	ctrl	○	●	●	○	○	○	○	67	3.2			●	In-Band Exchange
P11	pre2	○	○	○	●	●	●	●	45	3.1	●	●	●	-
P12	ctrl	○	○	○	●	●	●	●	34	3.8	●	●	●	-
P13	pre1	○	●	○	●	○	○	●	52	3.4	●	●	●	Gambling
P14	ctrl	○	○	○	●	●	○	●	41	5.2	●	●	●	-
P15	pre2	○	○	○	●	●	○	○	42	2.3	●	●	●	-
P16	ctrl	○	○	○	●	●	○	●	36	4.3	●	●	●	-
P17	pre1	○	○	○	○	●	●	●	47	3.1	●	●	●	-
P18	ctrl	○	○	○	○	●	○	●	32	2.3	●	●	●	-

TABLE 3.4: Overview of the scenario results of the second study participants. Each "●" represents that the participant did what is depicted in the column, e.g., sent the data or tried a method. The column "Anne's IdPs" marks which IdPs were requested by the participants. The providers are abbreviated (**A**mnesty, **F**acebook, **G**mail, **T**witter). The $*$ marks the participant that only continued the scenario after the researcher intervened. This, the other participants, and the reasons for failure are discussed in Section 3.4.3. "ATI" stands for Affinity for Technology Interaction Scale [70].

In-Band Safety Number Comparison The most common pitfall for the participants was anchoring their trust in publicly known information. Within that category, the participants often did an in-band exchange of the safety numbers.

P8 saw mismatches in the authentication ceremonies and asked Amira for her postal address and parts of the safety number. They decided that this was secret enough and sent the data. However, in the SOAP case, P8 stayed safe and decided against Anne because of an incorrect SOAP response.

P9 also saw the mismatches (QR, SOAP, safety number) but did not decide to stop and tried to find a way to communicate securely. They asked Michael why the scan failed. Michael said he reinstalled Signal and suggested sending the current safety number. P9 agreed, compared, and marked the conversation as verified. After that, they tried to determine whether Amira was actually Amira by asking whether Amira knew them. They assumed that they had met when they exchanged business cards. Amira claimed to remember Alex and sent the new safety number within that communication. P9 also asked for the work address on the business card, and Amira reported the correct one. After that, Amira was marked as verified.

P9 saw the SOAP mismatch and asked Anne for a different way to verify her. Anna sent the current safety number, but P9 was not entirely convinced, even though they marked Anna as verified. They noticed that some social media profiles were still unanswered. At that point, P9 ran out of time and decided to send the material to Amira and Michael verbally by telling the researcher.

P10 was rather insecure and initially seemed overwhelmed by the scenario. They initially wanted to look at the data they received from Hannah, but as they had never used Android before, they got lost in the data management and needed help from the researcher to go back to Signal. They were told again that they did not need to look at the data for the scenario. They did not know what they should compare for Amira but managed to scan the QR code for Michael and recognize that this failed. Then they told Michael they had sensible data and asked whether he could verify himself. Michael answered with the safety number. At first, P10 was not sure how to compare the numbers but, after a while, realized that the sent number matched the security number in the settings. Afterward, the same happens with Amira. Anna was also asked for verification, but the scenario time was up.

P6 saw the mismatch for the QR code, safety number, and SOAP after requesting them. They asked Amira and Michael why the numbers were not correct. Both sent the current number, and both received the data afterward. P6 told Anne that Signal said it was not secure to communicate based on the failed SOAP text. They even sent a screenshot when Anne said that this was not the case for her but did not send the data.

P3: Clicking Before Reading P3 was in the pre-registered SOAP condition. They saw a SOAP response without a request when they started a new chat with Anne. They clicked on "Mark Anne as verified" and sent her the data without recognizing this action. After the interview, in which they stated that Anne had already been verified, they were presented with the video and were surprised that they had actually clicked a button. They sent a SOAP request to Amira and Michael after seeing that they had to send a message for the other methods to work. They saw the faulty responses and deleted the chats afterward.

P13: Gambling for Money P13 was not sure who to send or not send the data to. After the time was up, they gambled and sent the data to Amira in the hope of getting more money. Although this is clearly related to the study design, we think it highlights that it was not clear to the participants what the secure and correct way to behave in this scenario was. On a similar note, another participant mentioned during the scenario and the interview that they thought it was strange that all the journalists were unsafe to send data to. They compared it to an exam situation where it seemed strange that all the questions had the same answer. Nevertheless, this participant behaved correctly. It seems that some participants required a strong will to abort the communication.

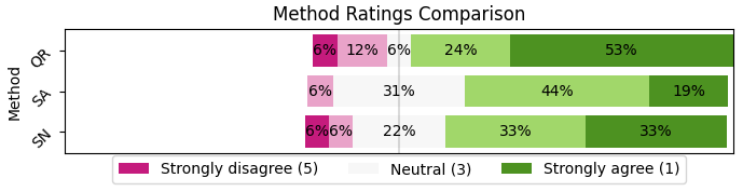
P2: Emotional Stress P2 initially decided not to contact any journalists, fearing that even sending a message would be too much. After the researcher intervened to tell them it would be all right, P2 went further. They saw the QR code mismatch and decided against SOAP requests, as they assumed they had to send an email, and ended up confused. The participant read through the FAQs for safety numbers and ultimately decided to mark every journalist as verified, although they expressed being unsure of whether that was correct. Afterward, P2 sent the data. The participant was clearly highly emotional and unsecure at that stage. In the interview, the participant expressed frustration with their decision but stated they were emotional in the situation and could not think clearly.

Study Conditions: Pre-Registered SOAP

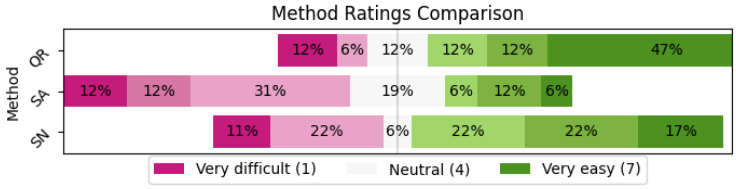
We could only identify one obvious case where the condition negatively affected the results. Pre-registered SOAP failed once as P3 auto-clicked the decision. We think an obstacle, e.g., a time restriction or a different visualization, could have prevented that. Only two participants decided to send Anne the data, and they covered both conditions. Although the text clearly indicated something was wrong, six out of nine participants directly sent another SOAP request, and one participant asked the person directly what was happening. Only one participant did not communicate further with Anne.

Quantitative Data - Perception

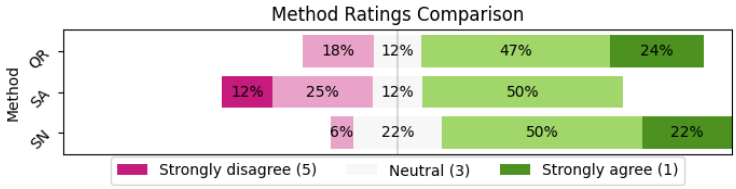
It is difficult to compare the results with those from Vaziripour et al. [210] due to different scenarios, methods, and UIs. Nonetheless, with only their and our studies about SA available, we think it is sensible to point out similarities and differences between them. The tested scenario in our study involved no direct human contact, e.g., via phone or in person, for verification. This was different in Vaziripour et al.'s study [210]. The researchers found that their proposal of SA ranked higher than the other available methods in the Single-ease-question (SEQ). Conversely, we observed that the tested implementation of SOAP ranked lower than the other two methods provided (see Figure 3.2b in the Appendix). Potentially in relation to the other available methods, SA ranked much lower in Vaziripour et al.'s study in the trust score than the other extremely high-ranking methods. We observed a mix of perceptions (see Figure 3.2c). The participants in our study generally trusted all the methods less than the participants in Vaziripour et al.'s study [210]. However, SA still ranked the lowest in both studies. We also asked participants whether they were confident in the decision they made with the method and saw that SA, again, ranked third in this category while not having led to failure in the scenario.



(A) How confident were participants with their decision? (Q8)



(B) Single-ease-question (SEQ) ratings of the methods. (Q9)



(C) How much do the participants trust the method? (Q7)

FIGURE 3.2: Participants' ratings of the methods. The "n"s differ slightly because not each participant used all the methods. "SN" is short for "safety number" and "SA" is short for "social authentication".

3.5 Discussion

We conducted two lab studies with nine and 18 participants, respectively, to observe SA in an AC in a no-win attack scenario. In this section, we discuss our results from the perspective of our research questions and highlight observations.

RQ1 & RQ2: Resistance Against Impersonation Attacks - Detection and Reaction

This is the first study that observed a SA ceremony in an attack scenario. We were interested in how resistant SA would be against impersonation attacks. So, as a first step, we researched an attacker who used typo squatting attacks to impersonate the communication partners. With the second iteration of the UI, we were **successful in preventing typosquatting attacks for SA**, and almost no one failed with SOAP. While with the simple interface in the first study, four participants failed because of SOAP, only one participant failed in the second

study. In the second study, the UI heavily supported the participants in detecting mismatches when an identifier was given. We applied a strong, opinionated design, e.g., interpreting anything other than the requested identities as incorrect and reducing possible providers to a fixed list. That seemed to help, but we could not measure long-term effects in our setting.

The participants often tried one method, then tried another, changed the journalist, returned to the first, and sometimes retried a previous method. The participants' flow through the tasks was not linear. Not all the participants reacted as hoped to an incorrect SOAP response. Some of the **participants retried** SOAP after seeing an incorrect response or even tried further and asked via text for a way to authenticate the other person. We cannot say whether that is a study artifact or not. We think that this should be investigated in future studies and also kept in mind when designing studies and interfaces. The participants not aborting the communication does not necessarily reflect the hope that is connected to SA: an intuitive method for recognizing whether you are communicating with the right person.

The participants without any technical knowledge about what happened **concluded that something was wrong**, although they did not necessarily attribute this to a malicious actor, despite the explicit mention of them in the scenario. Inputting the identifier beforehand helped the automatic detection and, therefore, the automated decision. Based on our data, we do not know whether this can be expected in a real scenario. It is, e.g., unclear where users would source the identifiers from. Anecdotally, in the first study, a participant was unsure whether there were unique Facebook identifiers and where to find them. There are paths to help the user here, e.g., if the person's identifier is not known, external means can verify it afterward (e.g., seeing connections in a social graph or validation through a third site). We think there are many possibilities for how this can develop over time, and it is an important area for future work.

While we think what we observed is promising, the sample was too small to draw strong conclusions regarding resistance against impersonation attacks in the real world. Also, while the privacy implications seem non-trivial, if the identifier is known, it could be checked to see if it was present in an identity leak database [139].

Safety Numbers, on the other hand, did not seem to be resistant to impersonation attacks. While safety numbers were not the focus of the study, we want to highlight that some of the participants failed the scenario because they did an in-band exchange and comparison of key material. As safety numbers comparison is a currently available AC, this should be researched further, as well as whether this has a negative real-world impact. We suggest seeing whether some preventive action can be taken on the client side, e.g., by pattern matching and informing users when they attempt to exchange safety numbers via chat.

RQ3: Perception and the Role of the Identity Provider

Although only one participant in the second study made a mistake with SOAP, the participants were not as confident about their decisions with SOAP as with the other methods. The same trend existed for the perceived usability or trustworthiness of the method to verify their contact. However, the small failure rates contradict that perception. We argue that this could be a positive situation for SA. The usability aspect seems to be solvable, and the participants behaved as intended. But, for the other methods, they behaved insecurely but felt as confident as with SA, creating an "illusion of security" [105]. Regarding SOAP, the participants behaved as hoped in the scenario. Now, we need to improve the participants' confidence in their own judgment based on SOAP. We are not sure where the difference in the perception of the methods comes from. The sample was too small to make any sensible statistical inferences, but we think further research could investigate the phenomenon.

Further Observations

This section discusses themes beyond our research questions that we hope can provide researchers and practitioners with relevant insights.

Identification of the Person vs. Authentication of the Connection Similar to other studies [59], we observed that the participants did not fully understand how encryption works and, following this, what an attack would look like. We observed, e.g., the assumption that if you have the correct phone number, you will end up with the correct person. In combination with the theme of the "almighty hacker"(see Dechand et al. [59]), participants assumed there is nothing a user can do to protect their communication effectively. So, explaining to the participant that doing something is necessary to communicate with the correct person may be easier than explaining that something is necessary to prevent others from listening. In short, the mental models of Signal's functions did not seem to align enough with the technical reality to understand an attacker. Considering this, it is understandable why the participants fell back to using addresses and shared secrets, or something perceived as such, to identify the other person.

Protocol/UI Challenges

Multiple requests are not a problem for the protocol per se but can complicate the UI. When designing a protocol and the corresponding interface, designers should remember that the interaction may involve multiple, sometimes canceled, requests. For example, on the one hand, we wanted to make sure that no data would be sent with a failed request, but on the other hand, a typo in the expected identifier was possible and needed to be traceable (false-negative).

The study participants wanted to believe the other person was legitimate. They were looking for a way to send the data rather than a reason not to send it.

To get the safety number or to receive a SOAP response, a chat contact has to **communicate with the other party**. Depending on the scenario, this communication can be a problem, and participants may hesitate to communicate. If the server is trustworthy, one can reduce the friction here. However, if one also does not trust the server, this is still a problem to be solved. For future studies, communication can be explicitly allowed in the scenario to reduce participants' confusion. In the study, pre-registration led to one failure, but it also indicated that something was wrong.

Vaziripour et al. [210] concluded that the necessary infrastructure for SA "needs to be more trusted than social media companies". We observed that the participants wanted to ask for the journalists' working email addresses. Such **custom providers** are not intended by the (SOAP) protocol. Allowing custom providers also allowed typo attacks on the provider level, making everything even more complicated. It is necessary to determine whether the usage of SA can be reduced to a fixed set of providers, depending on the use case. For example, in a company, setting the list of providers could vary vastly from that of instant messaging for personal use. We suggest finding a way to allow additional, possibly ad-hoc selected providers without impacting security. With SOAP, Linker et al. [134] proposed an interactive communicative way to verify a person. Vaziripour et al. [210] proposed an asynchronous interaction with the public key to identify mapping made public. We simulated this in the pre-registered condition after we observed that participants hesitated to even write a single message before verifying a person. We think this hesitation will not appear in most scenarios, but for those where it matters, it solves a real problem. Therefore, we suggest investigating further how an asynchronous solution could be achieved or how the interactive solution can reduce friction.

Signal Specifics

Some observations made are highly specific to the Signal app and may spark discussions about the UI. Some participants were confused by the way the safety numbers were presented. If a user opens the safety number page, the numbers appear in an animation, giving the impression they would be generated there just in time and, therefore, would change every time the site is visited.

Signal has an option to use the camera from the start screen. The participants tried using this feature to scan the QR code of the safety number. Here, direct feedback that something was done incorrectly could have helped the participants. As safety numbers can be capsuled in a specific format, it would also be possible for the operating system or Signal to provide some information on what type of data might have been scanned.

Also, Signal allows safety numbers to be compared from the clipboard, but no participant was aware of that. When something that looks like a safety number appears within a chat, Signal can provide additional information, e.g., to prevent in-band comparison, but also enhance the sharing of fingerprints between contacts that are already verified. Similarly to Shirvanian et al. [180], we observed situations where the participants had to compare long numbers across multiple views, but that was not intended and insecure to do in our scenario.

3.6 Limitations

Conducting a lab study comes with limitations. In this section, we describe our attempts to mitigate them. Participants in a lab study may behave differently than they would in real life. For our study, this could have led to more interaction and attempts even if the participants thought they should stop. The reward and risk system we used is not the same as beeing a whistleblow and get caught by the government. But unlike previous studies, which had no risk, we offered a real tradeoff. However, it is still a role play, and we are unaware of the extend of the impact. The setting of a lab study might lead participants to continue because they think there must be a way. We made sure that participants were aware that all the connections were potentially insecure and no communication was also an option. Also, within the scenario, trying different methods to authenticate the journalists was unproblematic. Nonetheless, anecdotal feedback suggested that the participants believed and liked the scenario and tried to empathize with the situation. Signal is an existing app, and numbers and a QR code scan are known visualizations and techniques. SA was a new concept to the participants. We did not make an introduction or provide a training session as we wanted to gather initial impressions and first-contact usability. We think this highlights that in the second study, the participants did not fail because of SOAP. We had to pick a fixed set of providers. To not only rely on U.S.A.-based providers, we added Amnesty.org in the second study, although it does not offer an identity service that would currently work with SOAP. We do not believe any participant knew this technical detail. Due to a bug with Amira, some of the participants did not need to send a message to get the safety number. We saw that sending a message made the participants hesitant, but ultimately, they all decided that this was not a show-stopper.

3.7 Conclusion

To test whether a new social authentication protocol called SOAP is usable and secure when attacked, we implemented an interface, conducted two qualitative user studies with an attack scenario, and compared social authentication to textual and QR code authentication ceremonies. The participants took on the role

of whistleblowers and were tasked with verifying the identities of journalists. In the first study, three out of nine participants were caught by the government due to SOAP, but the interface developed for the second study reduced this number to one out of 18 participants. Our results indicate that social authentication can lead to more secure behavior compared to more traditional authentication ceremonies. We interpret this as a positive signal, as it provides evidence that protocols can be designed to fit users' understanding, at least partially, and so reduce mistakes.

3.8 Acknowledgements

We thank David Basin and Felix Linker for their valuable input and discussions about the protocol, interface, and scenario. We thank the BonnEconLab for helping us recruit participants for the second study. We thank the Werner Siemens-Stiftung (WSS) for their generous support of this project.

Chapter 4

Conclusion

Within this dissertation I presented two cases of software that were researched in four studies. The results of the user studies, covering the participants' perceptions, knowledge, and usage of software features were compared to the technical reality of said software. The studies contributed to the greater goal of learning what people understand about software and to what effect in the domain of privacy and security.

The first software was the Corona-Warn-App (CWA), the official German contact tracing app. In chapter 2.2, I presented a study conducted before the release of the App in 2020. Taking data from an online survey, my co-authors and I analyzed answers from 744 participants. The survey focused on what the participants thought about the app, how they thought it worked, and whether they intended to install it. I reported themes arising from those questions and tried to find relations between the themes. I found the participants had many false assumptions about the app, e.g., 30% thought the app would use location services, and 57% believed the Corona-Warn-App (CWA) would inform its users of nearby infected persons. Some of the participants had no real idea what the app would do, e.g., expressed by not knowing that it would warn users who possibly had an infection. I found that 50% intended to install the CWA, although this intention was not always positively connected to the features the app provided but also sometimes connected to the assumptions of it having certain features the app did not have. This means some of the participants were positively influenced to install the app because they overestimated its capabilities. The strongest factors in the analysis that related to the intention was not knowledge but perceptions, e.g., perceiving the app as a threat to one's privacy or that the government's decisions were trusted. It is unclear how trust based on facts can relate to the actual app when there are many misconceptions present. I think it is neither desirable that people install an app out of incorrect assumptions nor that they do not install it because of it. Therefore, in my opinion, the results of the study highlight how important user studies are and to act on them. Before the release, I could only measure intention, and as we know from the concept called intention-behavior gap, not every intention leads to action. I knew the gap most likely existed, but I did not know how big the gap was. So, after the release, I analyzed further 837 participants' answers (see Section 2.3). Based on

the previous study, I thought more people intended (50%) to install the app than did in the end (45,9%). Still, both numbers are higher than the actual installation numbers based on estimations from download statistics. Generally speaking, knowledge increased, and false assumptions decreased. I found that the reasons named by the participants for their decision shifted. They were more concrete, more based on personal usefulness estimations and technical problems. Privacy concerns were less often mentioned than in the first study. However, they were still a relevant factor. The participants who thought the app would threaten their privacy less often installed it. I also found that assumptions I thought to be a threat to privacy were not necessarily perceived as one, e.g., that the app somehow detects infected people nearby. Although I could measure a relevant increase in knowledge, the participants still had many misconceptions. This suggests that during a time, when it could have been beneficial for the app to know facts about the app, many people did not know basic facts, e.g., that it used Bluetooth. That a person who does not use an app is not informed about it seems plausible. While the CWA may be a special case, this could, to some extent, still apply here. The results from the two studies did not focus on this, so maybe those who installed the app were better informed about its functionality. Based on that we investigated users and non-users of the app a third time. This time, the focus was on a more complete picture of what participants thought to be a feature of the app. I found that users knew more than non-users. However, the difference was not as large as I did expect.

Throughout all these studies, we asked whether the participants were aware that the app was open source. In all studies, this was a question that confused the participants. Many did not know what to do with that statement, and some even thought this would make the app less secure. The assumptions of the technical functions, e.g., what technology the CWA used, were often incomplete or just incorrect. The results hint at the question of how to properly phrase questions, e.g., in a survey, as technically correct and incorrect and can be very close to each other and far from the participants understanding. Participants may not be aware of or distinguish between terms like “Contact Tracing”, “GPS”, “Location”, or “Satelite”.

I learned from the studies that, in this case, for people with basic misunderstandings, trust or the lack of it towards the CWA hardly can be based on technical knowledge. The details between the decentralized approach and the centralized approach lie in how and where encounter data are stored and risk calculation happens. If people draw no distinction between these concepts, the privacy preserving aspects cannot be understood. Although trust in proxies, meaning trusted entities that rate software, maybe a viable way for those who do not want or cannot learn the technicalities of the CWA, there are other possibilities, e.g., finding techniques that match the intuition.

The second case study that was presented in this dissertation was exactly that: An attempt to implement a usable authentication ceremony, meaning enabling a user to share public key material with a partner in an intuitive way to

authenticate the chat partner in a way that is intuitive. I investigated whether a new protocol proposal (SOAP) for authentication ceremonies could achieve that. The idea of SOAP was that users prove that they have access to a social media account and that this is something that people can understand, not only if it works but also if the connection is attacked. I developed an interface for the popular instant messaging app Signal and conducted two lab studies to improve the interface. The participants were tasked to role play a whistleblower and make sure that they authenticated the journalists to not get caught by surveillance. I started with one-third of the participants failing the task in the first study with a simple interface. With the improvements, only one in 18 failed in the second study, based on SOAP. Additionally, I reported problems with already established ceremonies, e.g., scanning a QR code or comparing a textual representation of the fingerprint, that the evidence suggests are related to a mismatch of how they work and what the participants assumed. With the lab studies, I provide a new baseline on which new authentication ceremonies can be measured. For this, I also proposed a study design template that is more realistic than those of previous studies. Based on the results, I provided suggestions on how to extend the protocol, how to or not to build a corresponding interface, and how current ceremonies can be improved.

I started this dissertation with the idea that it is necessary for users to understand the consequences of decisions for some techniques. With the studies about the CWA I summarize that the technological details that build the possibility of being privacy preserving were not always known by those the features aimed at. This did not necessarily lead to a negative perception of the app, as other factors influenced the perception additionally. In an ideal world, all potential users are aware of all necessary as well as positive and negative details, but for now, it seems important to have trusted entities that judge software for the users and to build technology that is more relatable. The study with the SOAP protocol showed that this could work in some areas.

Bibliography

[1] *"Vorbildlich gelaufen" -Chaos Computer Club lobt deutsche Corona-App*. https://www.zdf.de/nachrichten/politik/corona-app-launch-100.html. Accessed: February 17, 2021.

[2] *A flood of coronavirus apps are tracking us. Now it's time to keep track of them.* https://www.technologyreview.com/2020/05/07/1000961/launching-mittr-covid-tracing-tracker/. Accessed: July 22, 2022.

[3] *AIC vs. BIC*. https://www.methodology.psu.edu/resources/AIC-vs-BIC/. Accessed: June 09, 2021.

[4] Whistleblower Aid. *Become a Whistleblower*. en-US. https://whistlebloweraid.org/become-a-whistleblower/signal/. Accessed: 30 October 2023.

[5] Icek Ajzen. "The theory of planned behavior". In: *Organizational behavior and human decision processes* 50.2 (1991), pp. 179–211.

[6] Icek Ajzen. "The theory of planned behaviour: Reactions and reflections". In: *Psychology & health* 26.9 (2011), pp. 1113–1127.

[7] Mashari Alatawi and Nitesh Saxena. "SoK: An Analysis of End-to-End Encryption and Authentication Ceremonies in Secure Messaging Systems". In: *Proceedings of the 16th ACM Conference on Security and Privacy in Wireless and Mobile Networks*. WiSec '23. Guildford, United Kingdom: Association for Computing Machinery, 2023, pp. 187–201. ISBN: 9781450398596. DOI: 10.1145/3558482.3581773. URL: https://doi.org/10.1145/3558482.3581773.

[8] Raghad A. Alharbi, Faisal T. Altayyari, Farah S. Alamri, and Sultan A. Alharthi. "Pandemic-Driven Technology During COVID-19: Experiences of Older Adults". In: *Companion Publication of the 2021 Conference on Computer Supported Cooperative Work and Social Computing*. CSCW '21. New York, NY, USA: Association for Computing Machinery, Oct. 2021, pp. 5–9. ISBN: 978-1-4503-8479-7. DOI: 10.1145/3462204.3481769. URL: https://doi.org/10.1145/3462204.3481769 (visited on 10/13/2022).

[9] Samuel Altmann et al. "Acceptability of app-based contact tracing for COVID-19: Cross-country survey study". In: *JMIR mHealth and uHealth* 8.8 (2020), e19857.

[10] Leonardo Angelini et al. "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*. PETRA '19. Rhodes, Greece: Association for Computing Machinery, 2019, pp. 620–628. ISBN: 9781450362320. DOI: 10.1145/3316782.3322763. URL: https://doi.org/10.1145/3316782.3322763.

[11] *Anteil der Nutzer von Social Networks in Europa nach ausgewählten Ländern 2020*. https://de.statista.com/statistik/daten/studie/214663/umfrage/nutzung-von-social-networks-in-europa-nach-laendern/. Accessed: February 19, 2021.

[12] *Apple and Google partner on COVID-19 contact tracing technology*. https://www.apple.com/newsroom/2020/04/apple-and-google-partner-on-covid-19-contact-tracing-technology/. Accessed: July 20, 2022.

[13] Armis. *BlueBorne*. Armis. 2021. URL: https://www.armis.com/research/blueborne/#/technical.

[14] Steven Arzt, Andreas Poller, and Gisela Vallejo. "Tracing Contacts With Mobile Phones to Curb the Pandemic:Topics and Stances in People's Online Comments About the Official German Contact-Tracing App". In: *Extended Abstracts of the 2021 CHI Conference on Human Factors in Computing Systems*. New York, NY, USA: Association for Computing Machinery, 2021, pp. 1–7. ISBN: 9781450380959. URL: https://doi.org/10.1145/3411763.3451631.

[15] Patrik Bachtiger, Alexander Adamson, Jennifer K. Quint, and Nicholas S. Peters. "Belief of having had unconfirmed Covid-19 infection reduces willingness to participate in app-based contact tracing". en. In: *npj Digital Medicine* 3.1 (Nov. 2020). Number: 1 Publisher: Nature Publishing Group, pp. 1–7. ISSN: 2398-6352. DOI: 10.1038/s41746-020-00357-5. URL: https://www.nature.com/articles/s41746-020-00357-5.

[16] Lars Baumgärtner et al. "Mind the GAP: Security & Privacy Risks of Contact Tracing Apps". In: *2020 IEEE 19th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom)*. 2020 IEEE 19th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom). Dec. 2020, pp. 458–467. DOI: 10.1109/TrustCom50675.2020.00069.

[17] Britt E. Bente, Jan W. J. R. van 't Klooster, Maud A. Schreijer, Lea Berkemeier, Joris E. van Gend, Peter J. H. Slijkhuis, Saskia M. Kelders, and Julia E. W. C. van Gemert-Pijnen. "The Dutch COVID-19 Contact Tracing App (the CoronaMelder): Usability Study". In: *JMIR Formative Research* 5.3 (Mar. 26, 2021), e27882. DOI: 10.2196/27882. URL: https://formative.jmir.org/2021/3/e27882 (visited on 11/03/2021).

[18] Bild. *Was bei Fehlermeldungen der Corona-App zu tun ist*. Axel-Springer-Verlag. 2020. URL: https://www.bild.de/digital/smartphone-und-tablet/handy-und-telefon/falsche-region-fehlermeldungen-der-corona-warn-app-so-reagieren-sie-71575830.bild.html.

[19] Bundeszentrale für politische Bildung. *Stereotypisierungen von Jung und Alt in der Corona-Pandemie*. Bundeszentrale für politische Bildung. 2020. URL: https://www.bpb.de/shop/zeitschriften/apuz/generationen-2020/324487/stereotypisierungen-von-jung-und-alt-in-der-corona-pandemie/#footnote-target-14.

[20] *Bluetooth low energy*. https://developer.android.com/guide/topics/connectivity/bluetooth-le#permissions. Accessed: May 29, 2021.

[21] Victoria Böhm, Christian Wolff, Corinna Geiselhart, Eric Karl, and Nina Kleindienst. "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*. MuC '21: Mensch Und Computer 2021. Ingolstadt Germany: ACM, Sept. 5, 2021, pp. 330–337. ISBN: 978-1-4503-8645-6. DOI: 10.1145/3473856.3474017. URL: https://dl.acm.org/doi/10.1145/3473856.3474017 (visited on 10/07/2021).

[22] BPA. *Veröffentlichung der Corona-Warn-App*. https://www.bundesregierung.de/breg-de/service/archiv/veroeffentlichung-der-corona-warn-app-1760892. Accessed: 2023-07-14. 2020.

[23] Virginia Braun and Victoria Clarke. "Using thematic analysis in psychology". In: *Qualitative Research in Psychology* 3.2 (2006), pp. 77–101. DOI: 10.1191/1478088706qp063oa.

[24] Fabian Buder, Anja Dieckmann, Vladimir Manewitsch, Holger Dietrich, Caroline Wiertz, Aneesh Banerjee, Oguz A. Acar, and Adi Ghosh. *Adoption Rates for Contact Tracing App Configurations in Germany*. 2020.

[25] Statistisches Bundesamt. *Bevölkerung nach Nationalität und Geschlecht (Quartalszahlen)*. https://www.destatis.de/DE/Themen/Gesellschaft-Umwelt/Bevoelkerung/Bevoelkerungsstand/Tabellen/liste-zensus-geschlecht-staatsangehoerigkeit.html#616584. Accessed: 2024-02-28. 2023.

[26] *Bundesinnenminister: Corona-Warn-App erfüllt höchste Ansprüche an Sicherheit und Datenschutz*. https://www.bmi.bund.de/SharedDocs/kurzmeldungen/DE/2020/06/vorstellung-corona-warn-app.html. Accessed: February 17, 2021.

[27] Bundesregierung. *Veröffentlichung der Corona-Warn-App*. Bundesregierung. 2020. URL: https://www.bundesregierung.de/breg-de/suche/veroeffentlichung-der-corona-warn-app-1760892.

[28] Bundesregierung. *Wie funktioniert und was kann die Corona-Warn-App?* Bundesregierung. 2020. URL: https://www.bundesregierung.de/breg-de/themen/corona-warn-app/corona-warn-app-erklaerfilm-1758828.

[29] *Bundesregierung - Mythen und Falschmeldungen - Corona-Warn-App*. https://web.archive.org/web/20200616193256/https://www.bundesregierung.de/breg-de/themen/mythen-und-falschmeldungen/corona-app-falschmeldungen-1758136. Accessed: February 02, 2021.

[30] Deutscher Bundestag. *Neufassung des Infektionsschutzgesetzes beschlossen*. https://www.bundestag.de/dokumente/textarchiv/2022/kw36-de-infektionsschutzgesetz-903658. Accessed: 2023-07-21. 2022.

[31] Presse Bundestag. *Mehr als 130 Millionen Euro Kosten für die Corona-Warn-App*. Bundesregierung. 2022. URL: https://www.bundestag.de/presse/hib/kurzmeldungen-877736.

[32] Kenneth P. Burnham and David R. Anderson. "Multimodel inference: understanding AIC and BIC in model selection". In: *Sociological methods & research* 33.2 (2004), pp. 261–304.

[33] Nicky Case. *How Privacy-First Contact Tracing Works*. Accessed 23.01.2024. URL: https://github.com/DP-3T/documents/blob/master/public_engagement/cartoon/en/shortened_onepage.png.

[34] Marta Caserotti, Paolo Girardi, Alessandra Tasso, Enrico Rubaltelli, Lorella Lotto, and Teresa Gavaruzzi. "Joint analysis of the intention to vaccinate and to use contact tracing app during the COVID-19 pandemic". en. In: *Scientific Reports* 12.1 (Jan. 2022). Number: 1 Publisher: Nature Publishing Group, p. 793. ISSN: 2045-2322. DOI: 10.1038/s41598-021-04765-9. URL: https://www.nature.com/articles/s41598-021-04765-9 (visited on 10/24/2022).

[35] *China launches coronavirus 'close contact detector' app*. https://www.bbc.com/news/technology-51439401. Accessed: July 22, 2022.

[36] Clickworker. *AI Training Data and other Data Management Services*. https://www.clickworker.com/. Accessed: January 16, 2024.

[37] Chaos Computer Club. *CCC | Home*. CCC. 2022. URL: https://www.ccc.de/en/.

[38] Jacob Cohen. *Statistical Power Analysis for the Behavioral Sciences*. Lawrence Erlbaum Associates, 1988.

[39] European Commission. *How should my consent be requested?* https://commission.europa.eu/law/law-topic/data-protection/reform/rights-citizens/how-my-personal-data-protected/how-should-my-consent-be-requested_en. Accessed: 2024-01-03. 2024.

[40] *Contact tracing*. https://dictionary.cambridge.org/de/worterbuch/englisch/contact-tracing. Accessed: June 08, 2022.

[41] *Contact Tracing in the European Union: Public Health Management of Persons, Including Healthcare Workers, Who Have Had Contact with COVID-19 Cases – Fourth Update*. https://www.ecdc.europa.eu/en/covid-19-contact-tracing-public-health-management. Accessed: June 08, 2022.

[42] *Contact Tracing Joint Statement*. https://www.esat.kuleuven.be/cosic/sites/contact-tracing-joint-statement/. Accessed: July 22, 2022.

[43] *CoroBlog zur wissenschaftlichen Auswertung der Corona-Datenspende-App*. https://www.rki.de/DE/Content/InfAZ/N/Neuartiges_Coronavirus/Corona-Datenspende.html. Accessed: January 26, 2021.

[44] *Corona-Apps im Überblick – Digitale Informations- und Hilfsangebote*. https://www.zusammengegencorona.de/informieren/corona-warn-app/corona-apps-im-ueberblick/. Accessed: May 26, 2021.

[45] *Corona-Pandemie: Alles Wissenswerte rund um die Warn-App*. https://www.tagesschau.de/inland/faq-corona-tracing-app-101.html. Accessed: February 19, 2021.

[46] *Corona-Tracing-App: Offener Brief an Bundeskanzleramt und Gesundheitsminister*. https://www.ccc.de/de/updates/2020/corona-tracing-app-offener-brief-an-bundeskanzleramt-und-gesundheitsminister. Accessed: February 23, 2021.

[47] *Corona-Tracing: Bundesregierung denkt bei App um*. https://www.tagesschau.de/inland/coronavirus-app-107.html. Accessed: July 22, 2022.

[48] Corona-Warn-App. *Kennzahlen zur Corona-Warn-App*. Robert-Koch-Institut. 2020. URL: https://www.coronawarn.app/de/analysis/.

[49] The authors of the Corona-Warn-App open-source project. *Open-Source-Projekt Corona-Warn-App – FAQ*. 2022. URL: https://www.coronawarn.app/en/faq/.

[50] The authors of the Corona-Warn-App open-source project. *So funktioniert die App am besten*. Robert-Koch-Institut. 2022. URL: https://www.coronawarn.app/de/#howto.

[51] *Corona-Warn-App: Fragen und Antworten*. https://www.bundesregierung.de/breg-de/themen/corona-warn-app/corona-warn-app-faq-1758392. Accessed: February 23, 2021.

[52] *Corona-Warn-App: Fragen und Antworten*. https://www.verbraucherzentrale.de/wissen/digitale-welt/apps-und-software/coronawarnapp-fragen-und-antworten-zur-deutschen-tracingapp-47466. Accessed: February 17, 2021.

[53] *Corona-Warn-App: Github*. https://github.com/corona-warn-app. Accessed: February 17, 2021.

[54] *Corona-Warn-App: Wenige Infektionen gemeldet (released October 2, 2020)*. https://www.aerzteblatt.de/archiv/216016/Corona-Warn-App-Wenige-Infektionen-gemeldet. Accessed: February 22, 2021.

[55] *Coronavirus Disease (COVID-19): Contact Tracing*. https://www.who.int/news-room/questions-and-answers/item/coronavirus-disease-covid-19-contact-tracing. Accessed: June 28, 2022.

[56] Research group COSIC. *Contact Tracing Joint Statement*. https://www.esat.kuleuven.be/cosic/sites/contact-tracing-joint-statement/. Accessed: 2023-03-08. 2020.

[57] *COVID-19 and Your Health*. https://www.cdc.gov/coronavirus/2019-ncov/daily-life-coping/contact-tracing.html. Accessed: June 08, 2022.

[58] Bart Custers, Simone van der Hof, Bart Schermer, Sandra Appleby-Arnold, and Noellie Brockdorff. "Informed Consent in Social Media Use - The Gap between User Expectations and EU Personal Data Protection law". eng. In: *SCRIPTed: A Journal of Law, Technology and Society* 10.3 (2013), pp. 435–457. URL: https://heinonline.org/HOL/P?h=hein.journals/scripted10&i=437 (visited on 10/14/2022).

[59] Sergej Dechand, Alena Naiakshina, Anastasia Danilova, and Matthew Smith. "In Encryption We Don't Trust: The Effect of End-to-End Encryption to the Masses on User Perception". In: *2019 IEEE European Symposium on Security and Privacy (EuroS&P)*. June 2019, pp. 401–415. DOI: 10.1109/EuroSP.2019.00037.

[60] Samuel Dooley, Dana Turjeman, John P Dickerson, and Elissa M. Redmiles. "Field Evidence of the Effects of Privacy, Data Transparency, and pro-Social Appeals on COVID-19 App Attractiveness". In: *CHI Conference on Human Factors in Computing Systems*. CHI '22. New York, NY, USA: Association for Computing Machinery, 2022. ISBN: 978-1-4503-9157-3. DOI: 10.1145/3491102.3501869. URL: https://doi.org/10.1145/3491102.3501869.

[61] *DP3T - Decentralized Privacy-Preserving Proximity Tracing*. https://github.com/DP-3T/documents. Accessed: July 22, 2022.

[62] Serge Egelman, Marian Harbach, and Eyal Peer. "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*. CHI '16. San Jose, California, USA: Association for Computing Machinery, 2016, pp. 5257–5261. ISBN: 9781450333627. DOI: 10.1145/2858036.2858265. URL: https://doi.org/10.1145/2858036.2858265.

[63] *Einnahmen und Ausgaben privater Haushalte*. https://www.destatis.de/DE/Themen/Gesellschaft-Umwelt/Einkommen-Konsum-Lebensbedingungen/Einkommen-Einnahmen-Ausgaben/_inhalt.html. Accessed: May 29, 2020.

[64] Glen H Elder, Eliza K Pavalko, and Elizabeth Colerick Clipp. *Working with archival data: Studying lives*. Vol. 88. Thousand Oaks, California: Sage Publications, Inc., 1992.

[65] erdgeist. *Corona-Tracing-App: Offener Brief an Bundeskanzleramt und Gesundheitsminister*. https://www.ccc.de/de/updates/2020/corona-tracing-app-offener-brief-an-bundeskanzleramt-und-gesundheitsminister. Accessed: 2023-03-08. 2020.

[66] European Commission. *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance)*. 2016. URL: https://eur-lex.europa.eu/eli/reg/2016/679/oj.

[67] *Eventregistrierung in der Corona-Warn-App*. https://www.bundesregierung.de/breg-de/themen/coronavirus/corona-warn-app-version-2-0-1889868. Accessed: July 22, 2022.

[68] *Faktencheck: Nein, die Corona-Warn-App nutzt keine persönlichen Kontaktdaten*. https://correctiv.org/faktencheck/2020/06/25/nein-die-corona-warn-app-nutzt-keine-persoenlichen-kontaktdaten/. Accessed: February 17, 2021.

[69] Grace Fox, Trevor Clohessy, Lisa van der Werff, Pierangelo Rosati, and Theo Lynn. "Exploring the Competing Influences of Privacy Concerns and Positive Beliefs on Citizen Acceptance of Contact Tracing Mobile Applications". In: *Computers in Human Behavior* 121 (Aug. 2021), p. 106806. ISSN: 07475632. DOI: 10.1016/j.chb.2021.106806. URL: https://linkinghub.elsevier.com/retrieve/pii/S0747563221001291 (visited on 10/07/2021).

[70] Thomas Franke, Christiane Attig, and Daniel Wessel. "A Personal Resource for Technology Interaction: Development and Validation of the Affinity for Technology Interaction (ATI) Scale". en. In: *International Journal of Human–Computer Interaction* 35.6 (Apr. 2019), pp. 456–467. ISSN: 1044-7318, 1532-7590. DOI: 10.1080/10447318.2018.1456150. URL: https://www.tandfonline.com/doi/full/10.1080/10447318.2018.1456150 (visited on 04/18/2023).

[71] Deen Freelon. *ReCal2: Reliability for 2 Coders*. Deen Freelon. 2022. URL: http://dfreelon.org/utils/recalfront/recal2/.

[72] Deen Freelon. *ReCal3: Reliability for 3+ Coders*. Deen Freelon. 2022. URL: http://dfreelon.org/utils/recalfront/recal3/.

[73] Alisa Frik, Juliann Kim, Joshua Rafael Sanchez, and Joanne Ma. "Users' Expectations About and Use of Smartphone Privacy and Security Settings". In: *Proceedings of the 2022 CHI Conference on Human Factors in Computing Systems*. CHI '22. New Orleans, LA, USA: Association for Computing Machinery, 2022. ISBN: 9781450391573. DOI: 10.1145/3491102.3517504. URL: https://doi.org/10.1145/3491102.3517504.

[74] Jemima A. Frimpong and Stephane Helleringer. *Financial Incentives for Downloading COVID–19 Digital Contact Tracing Apps*. SocArXiv 9vp7x. Center for Open Science, June 2020. DOI: 10.31219/osf.io/9vp7x. URL: https://ideas.repec.org/p/osf/socarx/9vp7x.html.

[75] *Fünf Monate nach dem Start: Die Tücken der Corona-Warn-App*. https://www.tagesschau.de/inland/faq-corona-warn-app-101.html. Accessed: February 17, 2021.

[76] Eva Ganglbauer, Geraldine Fitzpatrick, and Rob Comber. "Negotiating Food Waste: Using a Practice Lens to Inform Design". In: *ACM Trans. Comput.-Hum. Interact.* 20.2 (May 2013). ISSN: 1073-0516. DOI: 10.1145/2463579.2463582. URL: https://doi.org/10.1145/2463579.2463582.

[77] Eva Gerlitz and Maximilian Häring. "Privacy Research on the Pulse of Time: COVID-19 Contact-Tracing Apps". en. In: *Human Factors in Privacy Research*. Ed. by Nina Gerber, Alina Stöver, and Karola Marky. Springer International Publishing, 2023, pp. 219–235. ISBN: 978-3-031-28643-8. DOI: 10.1007/978-3-031-28643-8_11. URL: https://doi.org/10.1007/978-3-031-28643-8_11.

[78] The Federal Government of Germany. *Corona-Warn-App Open Source Project*. https://www.coronawarn.app/en/. Accessed: 2023-07-14. 2023.

[79] The Federal Government of Germany. *Corona-Warn-App to go into hibernation mode*. https://www.bundesregierung.de/breg-en/news/corona-warn-app-hibernation-mode-2183644. Accessed: 2023-06-15. 2023.

[80] The Federal Government of Germany. *Privacy statement*. https://www.coronawarn.app/en/privacy/. Accessed: 2023-03-13. 2023.

[81] The Federal Government of Germany. *SB05: How many active users does the Corona-Warn-App have?* https://www.coronawarn.app/en/science/2022-03-03-science-blog-5/. Accessed: 2023-07-14. 2022.

[82] The Federal Government of Germany. *What personal data is stored in the app?* https://www.coronawarn.app/en/faq/results/#personal_data. Accessed: 2023-07-17. 2023.

[83] The Federal Government of Germany. *Why are we following an open-source approach?* https://www.coronawarn.app/en/faq/results/#why_oss. Accessed: 2023-07-17. 2023.

[84] The Federal Government of Germany. *Wie funktioniert und was kann die Corona-Warn-App*. https://www.bundesregierung.de/breg-de/themen/corona-warn-app/corona-warn-app-erklaerfilm-1758828. Accessed: 2023-03-08. 2020.

[85] GitHub. *[INFO] URSACHE: 9002, Etwas ist schiefgelaufen. Timeout - Issue 998*. GitHub. 2020. URL: https://github.com/corona-warn-app/cwa-app-android/issues/998.

[86] GitHub. *App closing immediately on start - Issue 1053*. GitHub. 2020. URL: https://github.com/corona-warn-app/cwa-app-android/issues/1053.

[87] GitHub. *Error Reason: 2001; App does not work anymore - Issue 968*. GitHub. 2020. URL: https://github.com/corona-warn-app/cwa-app-android/issues/968.

[88] GitHub. *Release 1.1.2*. GitHub. 2020. URL: https://github.com/corona-warn-app/cwa-app-ios/releases/tag/v1.1.2.

[89] GitHub. *Releases - Corona Warn App*. GitHub. 2020. URL: https://github.com/corona-warn-app/cwa-app-android/releases.

[90] *Google Exposure Notification Key Server*. https://google.github.io/exposure-notifications-server/server_functional_requirements.html. Accessed: May 28, 2021.

[91] The Federal Government. *How does the Corona-Warn-App work and what does it do?* https://www.bundesregierung.de/breg-de/themen/corona-warn-app/corona-warn-app-englisch/how-does-the-corona-warn-app-work-and-what-does-it-do--1758870. Accessed: 2023-07-14. 2020.

[92] Paul Graßl, Hanna Schraffenberger, Frederik Zuiderveen Borgesius, and Moniek Buijzen. "Dark and Bright Patterns in Cookie Consent Requests". In: *Journal of Digital Social Research* 3.1 (2021), pp. 1–38. DOI: 10.33621/jdsr.v3i1.54. URL: https://jdsr.se/ojs/index.php/jdsr/article/view/54.

[93] Thomas Gross. "Validity and Reliability of the Scale Internet Users' Information Privacy Concerns (IUIPC)". In: *Proceedings on Privacy Enhancing Technologies* 2021.2 (2021), pp. 235–258.

[94] M. Guillon and P. Kergall. "Attitudes and opinions on quarantine and support for a contact-tracing application in France during the COVID-19 outbreak". In: *Public health* 188 (2020), pp. 21–31.

[95] Siddharth Gulati, Sonia Sousa, and David Lamas. "Design, development and evaluation of a human-computer trust scale". en. In: *Behaviour & Information Technology* 38.10 (Oct. 2019), pp. 1004–1015. ISSN: 0144-929X, 1362-3001. DOI: 10.1080/0144929X.2019.1656779. URL: https://www.tandfonline.com/doi/full/10.1080/0144929X.2019.1656779 (visited on 07/05/2022).

[96] Handelsblatt. *Corona-Warn-App: Bundesregierung zahlte 7,5 Millionen Euro für Werbung*. Handelsblatt. 2020. URL: https://www.handelsblatt.com/technik/it-internet/werbekampagne-corona-warn-app-bundesregierung-zahlte-7-5-millionen-euro-fuer-werbung/26021070.html.

[97] Julie M. Haney and Wayne G. Lutters. “"It's Scary... It's Confusing... It's Dull": How Cybersecurity Advocates Overcome Negative Perceptions of Security”. In: *Fourteenth Symposium on Usable Privacy and Security*. SOUPS 2018. Baltimore, MD: USENIX Association, Aug. 2018, pp. 411–425. ISBN: 978-1-939133-10-6. URL: https://www.usenix.org/conference/soups2018/presentation/haney-perceptions.

[98] Marian Harbach, Markus Hettig, Susanne Weber, and Matthew Smith. “Using personal examples to improve risk communication for security & privacy decisions”. en. In: *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. Toronto Ontario Canada: ACM, Apr. 2014, pp. 2647–2656. ISBN: 978-1-4503-2473-1. DOI: 10.1145/2556288.2556978. URL: https://dl.acm.org/doi/10.1145/2556288.2556978 (visited on 10/14/2022).

[99] Eszter Hargittai, Elissa M. Redmiles, Jessica Vitak, and Michael Zimmer. “Americans' willingness to adopt a COVID-19 tracking app”. In: *First Monday* (2020).

[100] Maximilian Häring, Eva Gerlitz, Matthew Smith, and Christian Tiefenau. “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*. Hamburg Germany: ACM, Apr. 2023, pp. 1–16. ISBN: 978-1-4503-9421-5. DOI: 10.1145/3544548.3581537. URL: https://dl.acm.org/doi/10.1145/3544548.3581537.

[101] Maximilian Häring, Eva Gerlitz, Christian Tiefenau, Matthew Smith, Dominik Wermke, Sascha Fahl, and Yasemin Acar. “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)*. online: USENIX Association, Aug. 2021, pp. 77–98. ISBN: 978-1-939133-25-0. URL: https://www.usenix.org/conference/soups2021/presentation/acar.

[102] Maximilian Häring, Julia Angelika Grohs, Eva Tiefenau, Matthew Smith, and Christian Tiefenau. “Can Johnny be a whistleblower? A qualitative user study of a social authentication Signal extension in an adversarial scenario”. In: *Twentieth Symposium on Usable Privacy and Security (SOUPS 2024)*. Philadelphia, PA: USENIX Association, Aug. 2024, pp. 259–278. ISBN: 978-1-939133-42-7. URL: https://www.usenix.org/conference/soups2024/presentation/haring.

[103] Farkhondeh Hassandoust, Saeed Akhlaghpour, and Allen C. Johnston. "Individuals' privacy concerns and adoption of contact tracing mobile applications in a pandemic: A situational privacy calculus perspective". In: *Journal of the American Medical Informatics Association* (2020).

[104] Federal Ministry of Health. *COVID-19 vaccination dashboard*. https://impfdashboard.de/en/. Accessed: 2023-07-13. 2023.

[105] Amir Herzberg and Hemi Leibowitz. "Can Johnny finally encrypt?: evaluating E2E-encryption in popular IM applications". en. In: *Proceedings of the 6th Workshop on Socio-Technical Aspects in Security and Trust*. Los Angeles California: ACM, Dec. 2016, pp. 17–28. ISBN: 978-1-4503-4826-3. DOI: 10.1145/3046055.3046059. URL: https://dl.acm.org/doi/10.1145/3046055.3046059 (visited on 03/28/2023).

[106] Amir Herzberg, Hemi Leibowitz, Kent Seamons, Elham Vaziripour, Justin Wu, and Daniel Zappala. "Secure Messaging Authentication Ceremonies Are Broken". en. In: *IEEE Security & Privacy* 19.2 (Mar. 2021), pp. 29–37. ISSN: 1540-7993, 1558-4046. DOI: 10.1109/MSEC.2020.3039727. URL: https://ieeexplore.ieee.org/document/9303352/ (visited on 03/28/2023).

[107] Robert Hinch et al. "Effective Configurations of a Digital Contact Tracing App: A Report to NHSX". In: (), p. 29.

[108] Kai T Horstmann, Susanne Buecker, Julia Krasko, Sarah Kritzler, and Sophia Terwiel. "Who does or does not use the 'Corona-Warn-App'and why?" In: *European Journal of Public Health* 31.1 (2021), pp. 49–51.

[109] Laszlo Horvath, Susan Banducci, and Oliver James. "Citizens' Attitudes to Contact Tracing Apps". In: *Journal of Experimental Political Science* 9 (Sept. 2, 2020), pp. 1–13. ISSN: 2052-2630, 2052-2649. DOI: 10.1017/XPS.2020.30. URL: https://www.cambridge.org/core/product/identifier/S2052263020000305/type/journal_article (visited on 01/12/2021).

[110] Yue Huang, Borke Obada-Obieh, Elissa M. Redmiles, Satya Lokam, and Konstantin Beznosov. "COVID-19 Information-Tracking Solutions: A Qualitative Investigation of the Factors Influencing People's Adoption Intention". In: *ACM SIGIR Conference on Human Information Interaction and Retrieval*. CHIIR '22. New York, NY, USA: Association for Computing Machinery, 2022, pp. 12–24. ISBN: 978-1-4503-9186-3. DOI: 10.1145/3498366.3505756. URL: https://doi.org/10.1145/3498366.3505756.

[111] Gesellschaft für Informatik. *Startseite - Gesellschaft für Informatik e.V.* Gesellschaft für Informatik e.V. 2022. URL: https://gi.de/.

[112] Presse- und Informationsamt der Bundesregierung. *Corona-Warn-App: der Baukasten für Unterstützerinnen und Unterstützer*. Bundesregierung. 2022. URL: https://styleguide.bundesregierung.de/sg-de/basiselemente/programmmarken/corona-warn-app.

[113] Krishna Chaitanya Jagadeesh Simma, Andrea Mammoli, and Susan M Bogus. "Real-Time Occupancy Estimation Using WiFi Network to Optimize HVAC Operation". In: *Procedia Computer Science* 155 (2019). The 16th International Conference on Mobile Systems and Pervasive Computing (MobiSPC 2019),The 14th International Conference on Future Networks and Communications (FNC-2019),The 9th International Conference on Sustainable Energy Information Technology, pp. 495–502. ISSN: 1877-0509. DOI: https://doi.org/10.1016/j.procs.2019.08.069.

[114] Sakshi Jain, Neil Zhenqiang Gong, Sreya Basuroy, Juan Lang, Dawn Song, and Prateek Mittal. "New Directions in Social Authentication". en. In: *Proceedings 2015 Workshop on Usable Security*. San Diego, CA: Internet Society, 2015. ISBN: 978-1-891562-40-2. DOI: 10.14722/usec.2015.23002. URL: https://www.ndss-symposium.org/ndss2015/ndss-2015-usec-programme/new-directions-social-authentication (visited on 03/28/2023).

[115] Jack Jamieson, Daniel A. Epstein, Yunan Chen, and Naomi Yamashita. "Unpacking Intention and Behavior: Explaining Contact Tracing App Adoption and Hesitancy in the United States". In: *CHI Conference on Human Factors in Computing Systems*. CHI '22. New York, NY, USA: Association for Computing Machinery, 2022. ISBN: 978-1-4503-9157-3. DOI: 10.1145/3491102.3501963. URL: https://doi.org/10.1145/3491102.3501963.

[116] Carlos Jensen and Colin Potts. "Privacy Policies as Decision-Making Tools: An Evaluation of Online Privacy Notices". In: *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. CHI '04. Vienna, Austria: Association for Computing Machinery, 2004, pp. 471–478. ISBN: 1581137028. DOI: 10.1145/985692.985752. URL: https://doi.org/10.1145/985692.985752.

[117] Daniel N. Jones and Delroy L. Paulhus. "Introducing the Short Dark Triad (SD3): A Brief Measure of Dark Personality Traits". In: *Assessment* 21.1 (2014), pp. 28–41. DOI: 10.1177/1073191113514105.

[118] Gabriel Kaptchuk, Eszter Hargittai, and Elissa M. Redmiles. "How good is good enough for COVID19 apps? The influence of benefits, accuracy, and privacy on willingness to adopt". In: *arXiv preprint arXiv:2005.04343* (2020).

[119] Farzaneh Karegar, Ala Sarah Alaqra, and Simone Fischer-Hübner. "Exploring User-Suitable Metaphors for Differentially Private Data Analyses". In: *Eighteenth Symposium on Usable Privacy and Security (SOUPS 2022)*. Boston, MA: USENIX Association, Aug. 2022, pp. 175–193. ISBN: 978-1-939133-30-4. URL: https://www.usenix.org/conference/soups2022/presentation/karegar.

[120] Farzaneh Karegar, Nina Gerber, Melanie Volkamer, and Simone Fischer-Hübner. "Helping John to Make Informed Decisions on Using Social Login". In: *Proceedings of the 33rd Annual ACM Symposium on Applied Computing*. SAC '18. Pau, France: Association for Computing Machinery, 2018, pp. 1165–1174. ISBN: 9781450351911. DOI: 10.1145/3167132.3167259. URL: https://doi.org/10.1145/3167132.3167259.

[121] Farzaneh Karegar, John Sören Pettersson, and Simone Fischer-Hübner. "The Dilemma of User Engagement in Privacy Notices: Effects of Interaction Modes and Habituation on User Attention". In: *ACM Trans. Priv. Secur.* 23.1 (Feb. 2020). ISSN: 2471-2566. DOI: 10.1145/3372296. URL: https://doi.org/10.1145/3372296.

[122] *Kennzahlen zur Corona-Warn-App*. https://www.rki.de/DE/Content/InfAZ/N/Neuartiges_Coronavirus/WarnApp/Archiv_Kennzahlen/Kennzahlen_28052021.pdf?__blob=publicationFile. Accessed: June 1, 2021.

[123] Keybase. *Keybase Book*. en-US. https://book.keybase.io/docs/server#meet-your-sigchain-and-everyone-elses. Accessed: 8 January 2024.

[124] Genia Kostka and Sabrina Habich-Sobiegalla. "In Times of Crisis: Public Perceptions Towards COVID-19 Contact Tracing Apps in China, Germany and the US". In: *Germany and the US (September 16, 2020)* (2020).

[125] Marvin Kowalewski et al. "52 Weeks Later: Attitudes Towards COVID-19 Apps for Different Purposes Over Time". In: *Proc. ACM Hum.-Comput. Interact.* 7.CSCW2 (Oct. 2023). DOI: 10.1145/3610042. URL: https://doi.org/10.1145/3610042.

[126] Anastasia Kozyreva, Philipp Lorenz-Spreen, Stephan Lewandowsky, Paul M. Garrett, Stefan M. Herzog, Thorsten Pachur, and Ralph Hertwig. "Psychological Factors Shaping Public Responses to COVID-19 Digital Contact Tracing Technologies in Germany". In: *Scientific Reports* 11.1 (1 Sept. 21, 2021), p. 18716. ISSN: 2045-2322. DOI: 10.1038/s41598-021-98249-5. URL: https://www.nature.com/articles/s41598-021-98249-5 (visited on 11/03/2021).

[127] Oksana Kulyk, Lauren Britton-Steele, Elda Paja, Melanie Duckert, and Louise Barkhuus. "#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". In: *Proc. ACM Hum.-Comput. Interact.* 6.MHCI (Sept. 2022). DOI: 10.1145/3546739. URL: https://doi.org/10.1145/3546739.

[128] Wassili Lasarov. "Im Spannungsfeld zwischen Sicherheit und Freiheit". In: *HMD Praxis der Wirtschaftsinformatik* (2020), pp. 1–18.

[129] Dominik Lauck. *FAQ: So funktioniert die Warn-App*. https://www.tagesschau.de/inland/faq-corona-tracing-app-103.html. Accessed: 2023-07-17. 2020.

[130] Sean Lawlor Lewi Kevin. *Deploying key transparency at WhatsApp*. en-US. Apr. 2023. URL: https://engineering.fb.com/2023/04/13/security/whatsapp-key-transparency/ (visited on 05/03/2023).

[131] Tianshi Li, Camille Cobb, Sagar Baviskar, Yuvraj Agarwal, Beibei Li, Lujo Bauer, Jason I. Hong, et al. "What Makes People Install a COVID-19 Contact-Tracing App? Understanding the Influence of App Design and Individual Difference on Contact-Tracing App Adoption Intention". In: *arXiv preprint arXiv:2012.12415* (2020).

[132] Tianshi Li, Cori Faklaris, Jennifer King, Yuvraj Agarwal, Laura Dabbish, Jason I. Hong, et al. "Decentralized is not risk-free: Understanding public perceptions of privacy-utility trade-offs in COVID-19 contact-tracing apps". In: *arXiv preprint arXiv:2005.11957* (2020).

[133] Guardian News & Media Limited. *How to contact the guardian securely*. https://www.theguardian.com/help/ng-interactive/2017/mar/17/contact-the-guardian-securely. Accessed: 30 October 2023.

[134] Felix Linker and David Basin. *SOAP: A Social Authentication Protocol*. 2024. arXiv: 2402.03199 [cs.CR].

[135] Lee Livsey, Helen Petrie, Siamak F. Shahandashti, and Aidan Fray. "Performance and Usability of Visual and Verbal Verification of Word-Based Key Fingerprints". en. In: *Human Aspects of Information Security and Assurance*. Ed. by Steven Furnell and Nathan Clarke. Vol. 613. Series Title: IFIP Advances in Information and Communication Technology. Cham: Springer International Publishing, 2021, pp. 199–210. ISBN: 978-3-030-81110-5. DOI: 10.1007/978-3-030-81111-2_17. URL: https://link.springer.com/10.1007/978-3-030-81111-2_17 (visited on 04/03/2023).

[136] L. Lohmeier. *Anzahl der Downloads der Corona-Warn-App über den Apple App Store und den Google Play Store (kumuliert) in Deutschland von Juni 2020 bis April 2023*. https://de.statista.com/statistik/daten/studie/1125951/umfrage/downloads-der-corona-warn-app/. Accessed: 2023-07-14. 2023.

[137] Xi Lu, Tera L. Reynolds, Eunkyung Jo, Hwajung Hong, Xinru Page, Yunan Chen, and Daniel A. Epstein. "Comparing Perspectives Around Human and Technology Support for Contact Tracing". In: *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*. CHI '21. Yokohama, Japan: Association for Computing Machinery, 2021. ISBN: 9781450380966. DOI: 10.1145/3411764.3445669. URL: https://doi.org/10.1145/3411764.3445669.

[138] Dominique Machuletz and Rainer Böhme. "Multiple Purposes, Multiple Problems: A User Study of Consent Dialogs after GDPR". In: *Proceedings on Privacy Enhancing Technologies* 2020.2 (2020), pp. 481–498. DOI: 10.2478/popets-2020-0037. URL: https://doi.org/10.2478/popets-2020-0037.

[139] Timo Malderle, Matthias Wübbeling, Sven Knauer, Arnold Sykosch, and Michael Meier. "Gathering and analyzing identity leaks for a proactive warning of affected users". In: *Proceedings of the 15th ACM International Conference on Computing Frontiers*. CF '18. Ischia, Italy: Association for Computing Machinery, 2018, pp. 208–211. ISBN: 9781450357616. DOI: 10.1145/3203217.3203269.

[140] Marta Malesza, Paweł Ostaszewski, Susanne Büchner, and Magdalena Claudia Kaczmarek. "The Adaptation of the Short Dark Triad Personality Measure – Psychometric Properties of a German Sample". In: *Current Psychology* 38.3 (June 2019), pp. 855–864. ISSN: 1936-4733. DOI: 10.1007/s12144-017-9662-0. URL: https://doi.org/10.1007/s12144-017-9662-0.

[141] Naresh K. Malhotra, Sung S. Kim, and James Agarwal. "Internet Users' Information Privacy Concerns (IUIPC): The Construct, the Scale, and a Causal Model". In: *Information Systems Research* 15.4 (2004), pp. 336–355. ISSN: 10477047, 15265536. URL: http://www.jstor.org/stable/23015787.

[142] Aleecia M Mcdonald and Lorrie Faith Cranor. "The Cost of Reading Privacy Policies". en. In: 4 (2009), p. 26.

[143] Yannic Meier, Judith Meinert, and Nicole C. Krämer. "Investigating Factors That Affect the Adoption of COVID-19 Contact-Tracing Apps: A Privacy Calculus Perspective." In: *Technology, Mind, and Behavior* 2.3 (Aug. 30, 2021), pp. 1–10. ISSN: 2689-0208. DOI: 10.1037/tmb0000040. URL: https://tmb.apaopen.org/pub/i7moqr3r (visited on 11/04/2021).

[144] Marcela S. Melara, Aaron Blankstein, Joseph Bonneau, Edward W. Felten, and Michael J. Freedman. "CONIKS: Bringing Key Transparency to End Users". In: *24th USENIX Security Symposium (USENIX Security 15)*. Washington, D.C.: USENIX Association, Aug. 2015, pp. 383–398. ISBN: 978-1-939133-11-3. URL: https://www.usenix.org/conference/usenixsecurity15/technical-sessions/presentation/melara.

[145] Fabiane Morgado, Juliana Meireles, Clara Neves, Ana Amaral, and Maria Ferreira. "Scale development: Ten main limitations and recommendations to improve future research practices". In: *Psicologia: Reflexão e Crítica* 30.1 (Jan. 2018). DOI: 10.1186/s41155-016-0057-1.

[146] moxie0. *Safety number updates*. https://signal.org/blog/safety-number-updates/. Accessed: 2 January 2024. Signal.

[147] Paul Mozur, Raymond Zhong, and Aaron Krolik. *In Coronavirus Fight, China Gives Citizens a Color Code, With Red Flags*. https://www.nytimes.com/2020/03/01/business/china-coronavirus-surveillance.html. Accessed: September 26, 2022. Mar. 2, 2020.

[148] Simon Munzert, Peter Selb, Anita Gohdes, Lukas F. Stoetzer, and Will Lowe. "Tracking and Promoting the Usage of a COVID-19 Contact Tracing App". In: *Nature Human Behaviour* 5.2 (2 Feb. 2021), pp. 247–255. ISSN: 2397-3374. DOI: 10.1038/s41562-020-01044-x. URL: https://www.nature.com/articles/s41562-020-01044-x (visited on 11/03/2021).

[149] Midas Nouwens, Ilaria Liccardi, Michael Veale, David Karger, and Lalana Kagal. "Dark Patterns after the GDPR: Scraping Consent Pop-Ups and Demonstrating Their Influence". In: *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*. CHI '20. New York, NY, USA: Association for Computing Machinery, 2020, pp. 1–13. ISBN: 9781450367080. DOI: 10.1145/3313831.3376321. URL: https://doi.org/10.1145/3313831.3376321.

[150] Patrick Howell O'Neilla. *No, coronavirus apps don't need 60% adoption to be effective*. https://www.technologyreview.com/2020/06/05/1002775/covid-apps-effective-at-less-than-60-percent-download/. Accessed: July 22, 2022.

[151] Michael E. O'Callaghan et al. "A national survey of attitudes to COVID-19 digital contact tracing in the Republic of Ireland". In: *Irish Journal of Medical Science* (2020), pp. 1–25.

[152] Cliodhna O'Connor and Helene Joffe. "Intercoder Reliability in Qualitative Research: Debates and Practical Guidelines". In: *International Journal of Qualitative Methods* 19 (2020), p. 1609406919899220. DOI: 10.1177/1609406919899220. URL: https://doi.org/10.1177/1609406919899220.

[153] Jonathan A. Obar and Anne Oeldorf-Hirsch. "The biggest lie on the Internet: ignoring the privacy policies and terms of service policies of social networking services". en. In: *Information, Communication & Society* 23.1 (Jan. 2020), pp. 128–147. ISSN: 1369-118X, 1468-4462. DOI: 10.1080/1369118X.2018.1486870. URL: https://www.tandfonline.com/doi/full/10.1080/1369118X.2018.1486870 (visited on 10/14/2022).

[154] *Offener Brief: Geplante Corona-App ist höchst problematisch*. http://www.fiff.de/presse/coronaappproblematisch. Accessed: January 28, 2021.

[155] Heise Online. *Zero Rating: Mobilfunk-Provider berechnen keinen Traffic für Corona-Warn-App*. Heise Medien GmbH & Co. KG. 2020. URL: https://www.heise.de/news/Zero-Rating-Mobilfunk-Provider-berechnen-keinen-Traffic-fuer-Corona-Warn-App-4785202.html.

[156] ZEIT ONLINE. *Appell an potenzielle Whistleblower*. https://www.zeit.de/administratives/2019-01/technologiebranche-whistleblower-suche. Accessed: 30 October 2023.

[157] *Open-Source-Projekt Corona-Warn-App – FAQ*. https://www.coronawarn.app. Accessed: June 08, 2022.

[158] *Pan-European Privacy-Preserving Proximity Tracing*. https://web.archive.org/web/20200409221119/https://www.pepp-pt.org/. Accessed: July 22, 2022.

[159] *Pan-European Privacy-Preserving Proximity Tracing*. https://github.com/pepp-pt/pepp-pt-documentation/blob/master/10-data-protection/PEPP-PT-data-protection-information-security-architecture-Germany.pdf. Accessed: January 22, 2021.

[160] Charlie Pinder, Jo Vermeulen, Benjamin R. Cowan, and Russell Beale. "Digital Behaviour Change Interventions to Break and Form Habits". In: *ACM Trans. Comput.-Hum. Interact.* 25.3 (June 2018). ISSN: 1073-0516. DOI: 10.1145/3196830. URL: https://doi.org/10.1145/3196830.

[161] *Pläne von Minister Spahn - Kritik an Corona-App wächst*. https://www.tagesschau.de/inland/corona-app-spahn-101.html. Accessed: January 28, 2021.

[162] The Washington Post. *Submit an Anonymous News Tip*. https://www.washingtonpost.com/anonymous-news-tips/. Accessed: 30 October 2023.

[163] *Poster: Positiv getestet? So teilen Sie Ihr Ergebnis über die Corona-Warn-App*. https://www.rki.de/DE/Content/InfAZ/N/Neuartiges_Coronavirus/WarnApp/Poster.pdf?__blob=publicationFile. Accessed: June 09, 2021.

[164] The Press and Information Office of the Federal Government. *Corona-Warn-App: Documentation*. Accessed 23.01.2024, author is the trademark owner of the logo. URL: https://github.com/corona-warn-app/cwa-documentation.

[165] *Pressemitteilung des Bundesministeriums für Gesundheit, des Bundesministeriums des Innern, für Bau und Heimat und des Bundeskanzleramts zum Projekt "Corona-App" der Bundesregierung*. https://www.bundesregierung.de/breg-de/aktuelles/pressemitteilung-des-bundesministeriums-fuer-gesundheit-des-bundesministeriums-des-innern-fuer-bau-und-heimat-und-des-bundeskanzleramts-zum-projekt-corona-app-der-bundesregierung-1747916. Accessed: January 28, 2021.

[166] *Privacy notice CWA*. https://www.coronawarn.app/assets/documents/cwa-privacy-notice-en.pdf. Accessed: February 23, 2021.

[167] *Publicly-available Exposure Notifications apps*. https://developers.google.com/android/exposure-notifications/apps. Accessed: July 29, 2022.

[168] *Qualtrics*. qualtrics.com. Accessed: January 22, 2021.

[169] Rainer Radtke. *Verteilung besorgniserregender Coronavirusvarianten (VOC) in Deutschland seit Februar 2022*. https://de.statista.com/statistik/daten/studie/1308508/umfrage/verteilung-von-corona-mutationen-in-deutschland/. Accessed: 2023-07-13. 2023.

[170] Elissa M. Redmiles. "User Concerns & Tradeoffs in Technology-Facilitated COVID-19 Response". In: *Digital Government: Research and Practice* 2.1 (Nov. 2020), pp. 1–12. ISSN: 2691-199X. DOI: 10.1145/3428093. URL: https://doi.org/10.1145/3428093.

[171] Jennifer Rigby and Bhanvi Satija. *WHO declares end to COVID global health emergency*. https://www.reuters.com/business/healthcare-pharmaceuticals/covid-is-no-longer-global-health-emergency-who-2023-05-05/. Accessed: 2023-06-15. 2023.

[172] *Risikogruppen sind überall*. https://de.statista.com/infografik/21145/groesse-von-ausgewaehlten-risikogruppen-in-deutschland/. Accessed: February 23, 2021.

[173] RKI. *COVID-19 Faelle 7-Tage-Inzidenz Deutschland*. https://github.com/robert-koch-institut/COVID-19_7-Tage-Inzidenz_in_Deutschland/blob/main/COVID-19-Faelle_7-Tage-Inzidenz_Deutschland.csv. Accessed: 2023-07-13. 2023.

[174] *RKI - The Institute*. https://www.rki.de/EN/Content/Institute/institute_node.html. Accessed: February 15, 2021.

[175] Leonie Schaewitz, David Lakotta, M. Angela Sasse, and Nikol Rummel. "Peeking Into the Black Box: Towards Understanding User Understanding of E2EE". In: *European Symposium on Usable Security*. EuroUSEC '21. Karlsruhe, Germany: Association for Computing Machinery, 2021, pp. 129–140. ISBN: 9781450384230. DOI: 10.1145/3481357.3481521. URL: https://doi.org/10.1145/3481357.3481521.

[176] Svenja Schröder, Markus Huber, David Wind, and Christoph Rottermanner. "When SIGNAL hits the Fan: On the Usability and Security of State-of-the-Art Secure Mobile Messaging". en. In: *Proceedings 1st European Workshop on Usable Security*. Darmstadt, Germany: Internet Society, 2016. ISBN: 978-1-891562-45-7. DOI: 10.14722/eurousec.2016.23012. URL: https://www.ndss-symposium.org/wp-content/uploads/2018/03/09-when-signal-hits-the-fan-on-the-usability-and-security-of-state-of-the-art-secure-mobile-messaging.pdf (visited on 03/28/2023).

[177] John S. Seberger and Sameer Patil. "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*. CHI '21. Yokohama, Japan: Association for Computing Machinery, 2021. ISBN: 9781450380966. DOI: 10.1145/3411764.3445485. URL: https://doi.org/10.1145/3411764.3445485.

[178] Muhammad Shahroz, Farooq Ahmad, Muhammad Shahzad Younis, Nadeem Ahmad, Maged N. Kamel Boulos, Ricardo Vinuesa, and Junaid Qadir. "COVID-19 digital contact tracing applications and techniques: A review post initial deployments". In: *Transportation Engineering* 5 (Sept. 2021), p. 100072. DOI: 10.1016/j.treng.2021.100072. URL: https://doi.org/10.1016/j.treng.2021.100072.

[179] Paschal Sheeran and Thomas L. Webb. "The Intention-Behavior Gap: The Intention-Behavior Gap". In: *Social and Personality Psychology Compass* 10.9 (Sept. 2016), pp. 503–518. ISSN: 17519004. DOI: 10.1111/spc3.12265. URL: https://onlinelibrary.wiley.com/doi/10.1111/spc3.12265 (visited on 02/09/2022).

[180] Maliheh Shirvanian, Nitesh Saxena, and Jesvin James George. "On the Pitfalls of End-to-End Encrypted Communications: A Study of Remote Key-Fingerprint Verification". In: *Proceedings of the 33rd Annual Computer Security Applications Conference*. ACSAC '17. New York, NY, USA: Association for Computing Machinery, Dec. 2017, pp. 499–511. ISBN: 978-1-4503-5345-8. DOI: 10.1145/3134600.3134610. URL: https://dl.acm.org/doi/10.1145/3134600.3134610 (visited on 03/28/2023).

[181] Signal. *Signal Messenger: Speak Freely*. Accessed 31.01.2024. URL: https://signal.org/.

[182] Lucy Simko, Jack L. Chang, Maggie Jiang, Ryan Calo, Franziska Roesner, and Tadayoshi Kohno. "COVID-19 Contact Tracing and Privacy: A Longitudinal Study of Public Opinion". In: *arXiv preprint arXiv:2012.01553* abs/2012.01553 (2020). DOI: 10.48550/arXiv.2012.01553. URL: https://doi.org/10.48550/arXiv.2012.01553.

[183] *Speeding up detection to slow down Ebola: Smartphone app is game-changer for contact tracing in hotspots in the Democratic Republic of the Congo*. https://www.afro.who.int/news/speeding-detection-slow-down-ebola-smartphone-app-game-changer-contact-tracing-hotspots. Accessed: July 22, 2022.

[184] Spiegel. *So erkennen Sie, ob Ihre Corona-App richtig funktioniert*. DER SPIEGEL GmbH & Co. KG. 2020. URL: https://www.spiegel.de/netzwelt/corona-warn-app-wann-die-app-auf-android-und-ios-vollstaendig-funktioniert-a-0088dfd8-d6b5-41d5-8855-513371dcb71f.

[185] Statista. *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. 2021. URL: https://de.statista.com/statistik/daten/studie/1125951/umfrage/downloads-der-corona-warn-app/.

[186] Statista. *Anzahl der Smartphone-Nutzer* in Deutschland in den Jahren 2009 bis 2021*. Statista. 2021. URL: https://de.statista.com/statistik/daten/studie/198959/umfrage/anzahl-der-smartphonenutzer-in-deutschland-seit-2010/.

[187] *Statistiken zur Smartphone-Nutzung in Deutschland*. https://de.statista.com/themen/6137/smartphone-nutzung-in-deutschland/. Accessed: February 23, 2021.

[188] Hanns Seidel Stiftung. *Zur Dynamik der Corona-Demonstrationen*. Hanns-Seidel-Stiftung e.V. 2020. URL: https://www.hss.de/publikationen/zur-dynamik-der-corona-demonstrationen-pub1703/.

[189] *Süddeutsche Zeitung GmbH*. https://sz.de/1.4850094. Accessed: February 25, 2021.

[190] Ben Swierzy, Markus Krämer, Daniel Vogel, Daniel Meyer, and Michael Meier. "Analyzing the Feasibility of Privacy-Respecting Automated Tracking of Devices Fleeing a Burglary". In: *2023 19th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob)*. 2023, pp. 452–459. DOI: 10.1109/WiMob58348.2023.10187747.

[191] *Sylvia Limmer: Corona-Appidemie stoppen!* https://www.afd.de/sylvia-limmer-corona-appidemie-stoppen/. Accessed: May 28, 2021.

[192] Tagesschau. *Corona-Warn-App: iPhone-Lücke war seit Wochen bekannt*. Norddeutscher Rundfunk. 2020. URL: https://www.tagesschau.de/investigativ/corona-warn-app-121.html.

[193] Tagesschau. *Ein Virus verändert die Welt*. https://www.tagesschau.de/faktenfinder/corona-chronik-pandemie-103.html. Accessed: 2023-07-13. 2020.

[194] Tagesschau. *Erster Coronavirus-Fall in Deutschland*. https://www.tagesschau.de/inland/coronavirus-deutschland-erster-fall-101.html. Accessed: 2023-07-13. 2020.

[195] Tagesschau. *Lücken bei Kontaktüberprüfung: Corona-App funktioniert auf iPhones fehlerhaft*. Norddeutscher Rundfunk. 2020. URL: https://www.tagesschau.de/investigativ/corona-warn-app-113.html.

[196] Tagesschau. *Pläne von Minister Spahn: Kritik an Corona-App wächst*. https://www.tagesschau.de/inland/corona-app-spahn-101.html. Accessed: 2023-03-08. 2020.

[197] Tagesschau. *tagesschau 20:00 Uhr, 25.07.2020*. Video. 2020. URL: https://www.youtube.com/watch?v=7zqLTA-1nHk.

[198] Joshua Tan, Lujo Bauer, Joseph Bonneau, Lorrie Faith Cranor, Jeremy Thomas, and Blase Ur. "Can Unicorns Help Users Compare Crypto Key Fingerprints?" en. In: *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems*. Denver Colorado USA: ACM, May 2017, pp. 3787–3798. ISBN: 978-1-4503-4655-9. DOI: 10.1145/3025453.3025733. URL: https://dl.acm.org/doi/10.1145/3025453.3025733 (visited on 12/11/2023).

[199] The Telegram Team. *Colorful Calls, Thanos Snap Effect, and an Epic Update for Bots*. https://telegram.org/blog/calls-and-bots. Accessed: 2 January 2024.

[200] Technologyreview. *No, coronavirus apps don't need 60% adoption to be effective*. MIT Technologyreview. 2020. URL: https://www.technologyreview.com/2020/06/05/1002775/covid-apps-effective-at-less-than-60-percent-download/.

[201] Telegram. *FAQ for the Technically Inclined*. en-US. https://core.telegram.org/techfaq#man-in-the-middle-attacks. Accessed: 8 January 2024.

[202] Rae Thomas, Zoe A Michaleff, Hannah Greenwood, Eman Abukmail, and Paul Glasziou. "Concerns and Misconceptions About the Australian Government's COVIDSafe App: Cross-Sectional Survey Study". en. In: *JMIR Public Health and Surveillance* 6.4 (Nov. 2020), e23081. ISSN: 2369-2960. DOI: 10.2196/23081. URL: http://publichealth.jmir.org/2020/4/e23081/ (visited on 02/15/2022).

[203] The New York Times. *Got a confidential news tip?* https://www.nytimes.com/tips. Accessed: 30 October 2023.

[204] Samuel Tomczyk, Simon Barth, Silke Schmidt, and Holger Muehlan. "Utilizing Health Behavior Change and Technology Acceptance Models to Predict the Adoption of COVID-19 Contact Tracing Apps: Cross-sectional Survey Study". In: *Journal of Medical Internet Research* 23.5 (May 19, 2021), e25447. DOI: 10.2196/25447. URL: https://www.jmir.org/2021/5/e25447 (visited on 11/04/2021).

[205] Simon Trang, Manuel Trenz, Welf H. Weiger, Monideepa Tarafdar, and Christy MK Cheung. "One app to trace them all? Examining app specifications for mass acceptance of contact-tracing apps". In: *European Journal of Information Systems* 29.4 (2020), pp. 415–428.

[206] *Transkript: Erklärfilm zur „Corona-Warn-App"*. https://www.bundesregierung.de/resource/blob/1726066/1760258/c4247487c176123b13003e6125ead7aa/2020-06-10-corona-warn-app-de-textversion-data.pdf. Accessed: February 17, 2021.

[207] UNESCO. *UNESCO | International Standard Classification of Education*. UNESCO. 2011. URL: http://uis.unesco.org/en/files/international-standard-classification-education-isced-2011-en-pdf.

[208] Christine Utz, Steffen Becker, Theodor Schnitzler, Florian M. Farke, Franziska Herbert, Leonie Schaewitz, Martin Degeling, and Markus Dürmuth. "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*. CHI '21. New York, NY, USA: Association for Computing Machinery, 2021. ISBN: 978-1-4503-8096-6. DOI: 10.1145/3411764.3445517. URL: https://doi.org/10.1145/3411764.3445517.

[209] Christine Utz, Martin Degeling, Sascha Fahl, Florian Schaub, and Thorsten Holz. "(Un)Informed Consent: Studying GDPR Consent Notices in the Field". In: *Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security*. CCS '19. New York, NY, USA: Association for Computing Machinery, 2019, pp. 973–990. ISBN: 9781450367479. DOI: 10.1145/3319535.3354212. URL: https://doi.org/10.1145/3319535.3354212.

[210] Elham Vaziripour, Devon Howard, Jake Tyler, Mark O'Neill, Justin Wu, Kent Seamons, and Daniel Zappala. "I Don't Even Have to Bother Them! Using Social Media to Automate the Authentication Ceremony in Secure Messaging". In: *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*. CHI '19. New York, NY, USA: Association for Computing Machinery, May 2019, pp. 1–12. ISBN: 978-1-4503-5970-2. DOI: 10.1145/3290605.3300323. URL: https://dl.acm.org/doi/10.1145/3290605.3300323 (visited on 03/28/2023).

[211] Elham Vaziripour, Justin Wu, Mark O'Neill, Jordan Whitehead, Scott Heidbrink, Kent Seamons, and Daniel Zappala. "Is that you, Alice? A Usability Study of the Authentication Ceremony of Secure Messaging Applications". In: *Thirteenth Symposium on Usable Privacy and Security (SOUPS 2017)*. Santa Clara, CA: USENIX Association, July 2017, pp. 29–47. ISBN: 978-1-931971-39-3. URL: https://www.usenix.org/conference/soups2017/technical-sessions/presentation/vaziripour.

[212] Elham Vaziripour et al. "Action Needed! Helping Users Find and Complete the Authentication Ceremony in Signal". In: *Fourteenth Symposium on Usable Privacy and Security (SOUPS 2018)*. Baltimore, MD: USENIX Association, Aug. 2018, pp. 47–62. ISBN: 978-1-939133-10-6. URL: https://www.usenix.org/conference/soups2018/presentation/vaziripour.

[213] Felix Velicia-Martin, Juan-Pedro Cabrera-Sanchez, Eloy Gil-Cordero, and Pedro R. Palos-Sanchez. "Researching COVID-19 tracing app acceptance: incorporating theory from the technological acceptance model". In: *PeerJ Computer Science* 7 (Jan. 2021), e316. ISSN: 2376-5992. DOI: 10.7717/peerj-

cs.316. URL: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7924669/ (visited on 07/14/2023).

[214] Verbraucherschutz. *Facebook & WhatsApp: Kettenbrief zu STOPCOVID-App – Stimmt das?* Verbraucherschutz. 2020. URL: https://www.verbraucherschutz.com/warnungsticker/facebook-whatsapp-kettenbrief-zu-stopcovid-app-stimmt-das/.

[215] *Veröffentlichung der Corona-Warn-App*. https://www.bundesregierung.de/breg-de/themen/coronavirus/veroeffentlichung-der-corona-warn-app-1760892. Accessed: February 01, 2021.

[216] *Version 1.11: Corona-Warn-App nun mit Kennzahlen zum Infektionsgeschehen*. https://www.coronawarn.app/de/blog/2021-01-28-corona-warn-app-version-1-11/. Accessed: February 15, 2021.

[217] My Villius Zetterholm, Yanqing Lin, and Päivi Jokela. "Digital Contact Tracing Applications during COVID-19: A Scoping Review about Public Acceptance". In: *Informatics* 8.3 (July 22, 2021), p. 48. ISSN: 2227-9709. DOI: 10.3390/informatics8030048. URL: https://www.mdpi.com/2227-9709/8/3/48 (visited on 11/03/2021).

[218] Michel Walrave, Cato Waeterloos, and Koen Ponnet. "Ready or Not for Contact Tracing? Investigating the Adoption Intention of COVID-19 Contact-Tracing Technology Using an Extended Unified Theory of Acceptance and Use of Technology Model". In: *Cyberpsychology, Behavior, and Social Networking* (2020).

[219] *Wann kommt die App, die hilft?* https://www.zeit.de/digital/datenschutz/2020-04/corona-app-tracking-handydaten-bluetooth-datenschutz. Accessed: February 19, 2021.

[220] *Washington Post-University of Maryland national poll, April 21-26, 2020*. https://web.archive.org/web/20200501144955if_/https://www.washingtonpost.com/context/washington-post-university-of-maryland-national-poll-april-21-26-2020/3583b4e9-66be-4ed6-a457-f6630a550ddf/. Accessed: February 10, 2021.

[221] *Wenn am nächsten Sonntag Bundestagswahl wäre ...* https://www.wahlrecht.de/umfragen/forsa.htm. Accessed: January 27, 2021.

[222] Caroline Wiertz, Aneesh Banerjee, Oguz A. Acar, and Adi Ghosh. "Predicted Adoption Rates of Contact Tracing App Configurations-Insights from a choice-based conjoint study with a representative sample of the UK population". In: *Available at SSRN 3589199* (2020).

[223] Simon N. Williams, Christopher J. Armitage, Tova Tampe, and Kimberly Dienes. "Public Attitudes towards COVID-19 Contact Tracing Apps: A UK-based Focus Group Study". In: *Health Expectations* 24.2 (Apr. 2021), pp. 377–385. ISSN: 1369-6513, 1369-7625. DOI: 10.1111/hex.13179. URL: https://onlinelibrary.wiley.com/doi/10.1111/hex.13179 (visited on 02/15/2022).

[224] Kantar Worldpanel. *Android vs. iOS*. https://www.kantarworldpanel.com/global/smartphone-os-market-share/. Accessed: 2022-08-11. 2022.

[225] Justin Wu, Cyrus Gattrell, Devon Howard, Jake Tyler, Elham Vaziripour, Daniel Zappala, and Kent Seamons. ""Something isn't secure, but I'm not sure how that translates into a problem": Promoting autonomy by designing for understanding in Signal". In: *Fifteenth Symposium on Usable Privacy and Security (SOUPS 2019)*. 2019, pp. 137–153.

[226] Justin Wu and Daniel Zappala. "When is a Tree Really a Truck? Exploring Mental Models of Encryption". In: *Fourteenth Symposium on Usable Privacy and Security (SOUPS 2018)*. Baltimore, MD: USENIX Association, Aug. 2018, pp. 395–409. ISBN: 978-1-939133-10-6. URL: https://www.usenix.org/conference/soups2018/presentation/wu.

[227] Viktor von Wyl et al. "Drivers of acceptance of COVID-19 proximity tracing apps in Switzerland". In: *medRxiv* (2020).

[228] Tarun Kumar Yadav, Devashish Gosain, Amir Herzberg, Daniel Zappala, and Kent Seamons. "Automatic Detection of Fake Key Attacks in Secure Messaging". In: *Proceedings of the 2022 ACM SIGSAC Conference on Computer and Communications Security*. CCS '22. Los Angeles, CA, USA: Association for Computing Machinery, 2022, pp. 3019–3032. ISBN: 9781450394505. DOI: 10.1145/3548606.3560588. URL: https://doi.org/10.1145/3548606.3560588.

[229] ZDF. *Chaos Computer Club lobt deutsche Corona-App*. ZDF. 2020. URL: https://web.archive.org/web/20211222145023/https://www.zdf.de/nachrichten/politik/corona-app-launch-100.html.

[230] ZDF. *Keine Hintergrundaktualisierung-Einstellung bei Warn-App: Was man wissen muss*. ZDF. 2020. URL: https://web.archive.org/web/20211113120146/https://www.zdf.de/nachrichten/digitales/coronavirus-warnapp-fehlfunktion-android-100.html.

[231] ZDF. *Probleme bei der Nutzung-Die vielen Fehlermeldungen der Corona-App*. ZDF. 2020. URL: https://web.archive.org/web/20210323025851/https://www.zdf.de/nachrichten/politik/corona-app-fehlermeldungen-102.html.

[232] Süddeutsche Zeitung. *So erreichen Sie das Investigativ-Team der Süddeutschen Zeitung*. https://www.sueddeutsche.de/projekte/kontakt/#messenger. Accessed: 30 October 2023.

[233] Baobao Zhang, Sarah Kreps, Nina McMurry, and R. Miles McCain. "Americans' perceptions of privacy and surveillance in the COVID-19 pandemic". In: *Plos one* 15.12 (2020), e0242652.

[234] Zusammengegencorona. *Fake-News rund um das Coronavirus*. Bundesministerium für Gesundheit. 2022. URL: https://www.zusammengegencorona.de/informieren/alltag-und-reisen/fake-news-rund-um-das-coronavirus/.

Appendix A

Appendix for "Never ever or no matter what"

A.1 Study Material

Englisch Survey (Translation)

Screening Questions

- Q1 What is your age?
  [Free Text]
- Q2 In which federal state do you live?
- Q3 Do you use a smartphone?
  [Yes, an Android / Yes, an IPhone / Yes, another smartphone / Yes, but I don't know which / No / I don't want to state]
- Q4 What is your netto household income?
  *[$<=$ 1300*e* / *1300-1700€/ 1700-2600€/ 2600-3600€/ 3600-5000€/* $>$ 5000*e* / *I don't want to state]*
- Q5 What is the number of individuals living in your household?
  [1 / 2 / 3 / 4 or more / I don't want to state]
- Q6 What is the highest-level vocational qualification you hold?
  [Completed apprenticeship / Other; Vocational qualification: / University degree / Master or Technician certification or equivalent technical school diploma / Vocational school diploma / Technical school diploma / No vocational qualification / Technical college degree (or engineering school diploma) / I don't want to state / Abitur (German university entrance qualification)]

App Description and Media Sources

The COVID-19 coronavirus pandemic is a worldwide problem. The Corona warning app for Germany is one of the measures planned to assist health authorities in tracing and containing infection, being developed by SAP to run on Deutsche Telekom infrastructure. The Robert Koch Institute (RKI) will publish the app when it is ready. It is also referred to as the 'Corona app', 'COVID app' or 'contact tracing app'.

- Q7 Have you heard of the plans for this app? If 'yes', please select where you heard about the app. Multiple selections possible.
  [Public broadcasters (ARD, ZDF, WDR, etc.) / Non-public TV (Pro7, Vox, N24, etc.) / Scientific publications / Newspapers, journals, magazines, etc. / Family member / Official government/state

agency websites (Robert Koch Institute, Federal Government, etc.) / Other websites: / I have not heard about this app / Friends / Social media (Twitter, Facebook, YouTube, TikTok, etc.) / Work colleagues/associates / Don't know/I don't want to state / Official Corona Warning App website

Knowledge

- Q8 Which of the below statements do you think will apply regarding the app? (please check all that apply.)
  - The app uses Bluetooth.
  - Through the app I can donate health data to the Robert Koch Institute for research purposes.
  - The app determines when other smartphones are nearby that are also using the app.
  - The app shares temporary IDs and timestamps.
  - The app enables the government to see my current location.
  - The app enables the government to see if people are not keeping a safe distance from others.
  - Usage of the app will be mandatory.
  - The app shares the names and phone numbers of my contacts with the government.
  - The app infringes my basic rights.
  - The app can be used to demonstrate to others that I am not currently COVID-19 positive.
  - The app facilitates decision-making on who should be tested for COVID-19.
  - The app shares fitness data.
  - The app can help fight the spread of the COVID-19 virus.
  - The app uses location services (like GPS).
  - The app shares a profile of my movement.
  - None of the above applies.
  - Don't know
  - The app undermines my privacy.
- Q9 What statements do you think apply regarding the app when other users are COVID-19 positive? (please check all that apply.)
  - The app enables the government to see if someone is not complying with quarantine orders.
  - The app notifies me if I have had contact with an individual who later tested positive for COVID-19.
  - The app notifies me when an infected person is located nearby.
  - None of the above applies.
  - Don't know
- Q10 What statements do you think apply regarding the app when you yourself are COVID-19 positive? (please check all that apply.)
  - The app informs other app users who have been close to me that they may have contracted the virus.

- The app sends data continuously to the RKI.
- A physician or the public health authority has to confirm my positive COVID-19 test result before the app sends data to the RKI.
- The app enables the government to see if I am not complying with quarantine orders.
- None of the above applies.
- Don't know

App Description and Comprehension

A brief introduction is provided below on the planned capabilities of the contact tracing app. The federal government intends to introduce a smartphone app to trace COVID-19 transmission in the near future. The app is to be very user-friendly and its usage voluntary. The app is designed to ensure that virus transmission is detected more quickly. This allows taking targeted containment measures.
When in use, the app determines what other users of the app are located near you. The app does this via Bluetooth. The app will alert you if you have been near someone within the past few days who subsequently tested positive for COVID-19. The app then informs you of what you need to do next, such as get tested for COVID-19.

- Q11 How will the described app determine what people have been near me?
  [Bluetooth / Location services (such as GPS) / My phone Contacts list / Don't know]

Install General

In answering the following questions, please imagine that the app described above has already been released. The app is being developed by SAP to run on Deutsche Telekom infrastructure. The Robert Koch Institute (RKI) is in charge of the app and evaluates the data. The exclusive permissible usage of the data is to fight COVID-19.

- Q12 How likely is it that you will use the app?
  [Definitely will use it / Probably will use it / Undecided / Probably will not use it / Definitely will not use it / Response declined / Don't know]
- Q13 What is the primary reason for your answer?
  [Free text]

Potential Properties

Q14 You will now be presented with 24 statements. These statements concern characteristics or things that **could** apply or be true with the app. Please select how these statements, **if true**, would influence your willingness to use the app.
[Definitely would use it / Probably would be willing to use it / No influence on my willingness / Probably would not be willing to use it / Definitely would not use it / Don't know]

- The government would be prevented by law, but not by technical means, from misusing the data for surveillance purposes.
- Using the app would enable the RKI to find out if I am not complying with minimum distancing to other individuals.
- The RKI would have a database with the contact data of infected individuals and the people they have had contact with.

- If I test positive for COVID-19, the app would allow the RKI to see who I had contact with in order to notify those individuals
- The German Federal Office for Information Security (BSI) would verify that the app fulfills data security and data protection requirements.
- Using the app would make possible a speedier return to normal public life.
- Technical measures would be implemented to ensure the data are protected.
- There is a possibility that the app could incorrectly report infection risk, resulting in me having to quarantine unnecessarily
- Using the app would help re-start the economy faster
- If the app notifies me that I may have been infected, I would have be required by law to quarantine.
- The app would notify me if I have been in a situation putting me at risk of contracting COVID-19.
- There is a possibility that the app could incorrectly report infection risk, resulting in me having to get tested unnecessarily
- Independent security experts would verify that the app fulfills data security and data protection requirements.
- The app would use information about my location to more accurately monitor infection risk for others
- Protection of the data would be guaranteed pursuant to a data protection policy and the General Data Protection Regulation.
- The app would not collect any data about my location.
- The app would inform people of infection risk who would not otherwise be contacted by the public health authority.
- Any nearby hackers could find out if I have tested positive for COVID-19.
- This question pertains to attentive completion of the survey. Please select "No influence" as response.
- If somebody near me has tested positive for COVID-19, the app would enable the RKI to see that I have had contact with that individual in order to notify me accordingly.
- Protection of the data would be guaranteed under a new law drafted especially for the app
- If I have tested positive for COVID-19, the app would automatically notify other users of the app who are at risk being exposed through contact with me
- The app would be open-source
- The app would support the RKI to better assess the COVID-19 situation.

It is being discussed whether use of the app should be made mandatory in certain situations where people come in contact in groups, such as patronizing restaurants or utilizing bus or train services, to facilitate targeted monitoring of infection risk. It must be considered however that roughly 20% of the German population would be excluded from using such services due to not having a smartphone.

- Q15 Would you approve or disapprove of such mandatory usage?
  [Approve entirely / Mainly approve / Neither approve nor disapprove / Mainly disapprove / Disapprove entirely / Response declined / Don't know]

Demographics

- Q16 What is your gender?
  [Male / Female / Non-binary / Would like to self-describe: / I don't want to state]
- Q17 What is your work status?
  [School student / University/college student / Employee / Civil servant / Self-employed / Freelancer / Unemployed / Retiree / I don't want to state]
- Q18 Do you have specialized computing skills, such as: system administration, programming, IT security, tech support, power user, etc?
  [Yes / No / I don't want to state]
- Q19 Please indicate your agreement or disagreement with the following: "I generally trust the government to do the right thing."
  [Fully agree / Mostly agree / Neither agree nor disagree / Mostly disagree / Fully disagree / I don't want to state]
- Q20 What party do you have the most affinity with?
  [The Greens / CDU/CSU / SPD / FDP / AfD / The Left / Others/I don't want to state]
- Q21 Currently, how frequently do you have close personal contact with people not from your household?
  [Once a week at most / A few times a week / A few times a day / Several times a day / I don't want to state]
- Q22 How concerned or unconcerned are you about COVID-19 in regard to the following three areas?
  Health, The economy, Society
  [Unconcerned / A bit concerned / Concerned / Very concerned / I don't want to state]
- Q23 Do you fall within a COVID-19 high-risk group?
  [Yes / No / Don't know / I don't want to state]
- Q24 Does someone close to you fall within a COVID-19 high-risk group?
  [Yes / No / Don't know / I don't want to state]
- Q25 Have you or any person close to you fallen ill with Covid-19?
  [Yes / No / Don't know / I don't want to state]
- Q26 Has anyone close to you died of Covid-19?
  [Yes / No / Don't know / I don't want to state]
- Q27 How has the Covid-19 pandemic affected you financially?
  [Positive impact / No impact / Negative impact / Critical impact / I don't want to state]
- Q28 Has the Covid-19 pandemic resulted in you having to look after/care for someone at home?
  [Yes / No / I don't want to state]
- Q29 How has the crisis affected your work?
  [Unaffected / Working from home / Short-time work / Became unemployed / Found employment / I don't want to state]

Thank you!

To find out more about the coronavirus and how to best protect yourself and your family, follow this link to the coronavirus info web pages of the Federal Center for Health Education: https://www.infektionsschutz.de/coronavirus/

Thank you very much for participating in this survey! You can enter any comments or your opinion on the app in the field below, or contact the survey administrators directly via e-mail.

German Survey (Original)

Screening Fragen

- Q1 Wie alt sind Sie?
  [Freitext]
- Q2 In welchem Bundesland wohnen Sie derzeit?
- Q3 Nutzen Sie ein Smartphone?
  [Ja, ein Android / Ja, ein IPhone / Ja, ein anderes / Ja, weiß aber nicht was für eins / Nein / Möchte ich nicht sagen]
- Q4 Was ist Ihr netto Haushaltseinkommen?
  [<= 1300e / 1300-1700€/ 1700-2600€/ 2600-3600€/ 3600-5000€/ > 5000e / Möchte ich nicht sagen]
- Q5 Wie viele Personen leben in Ihrem Haushalt?
  [1 / 2 / 3 / 4 oder mehr / Möchte ich nicht sagen]
- Q6 Was ist Ihr höchster beruflicher Abschluss?
  [Abgeschlossene Lehre / Anderen; beruflichen Ausbildungsabschluss, und zwar: / Hochschulabschluss / Meister-, Techniker- oder gleichwertiger Fachschulabschluss / Berufsfachschulabschluss / Fachschulabschluss / Keinen beruflichen Ausbildungsabschluss / Fachhochschulabschluss (auch Abschluss einer Ingenieurschule) / Möchte ich nicht sagen / Abitur]

App Beschreibung und Nachrichtenquellen

Die derzeitige Coronavirus-Pandemie („COVID-19") ist allgegenwärtig. Eine der geplanten Maßnahmen, um die Gesundheitsämter beim Nachverfolgen vom Infektionsgeschehen zu unterstützen, ist die Corona-Warn-App für Deutschland. Die App wird von SAP entwickelt. Die Deutsche Telekom betreibt die Infrastruktur. Nach Fertigstellung der App wird das Robert Koch-Institut (RKI) die App herausgeben. Diese App wird auch als Corona-App, COVID-App oder Contact-Tracing App bezeichnet.

- Q7 Haben Sie schon von der geplanten App gehört? Wenn ja, wählen Sie bitte aus, wo Sie Informationen über die App bekommen haben. Mehrfachauswahl möglich.
  [Öffentlich rechtliche Sender (ARD, ZDF, WDR, etc.) / Private Sender (Pro7, Vox, N24, etc.) / Wissenschaftliche Veröffentlichungen / Zeitungen, Zeitschriften, Magazine, etc. / Familie / Staatliche Webseiten (Robert Koch-Institut, Bundesregierung, etc.) / Webseiten, z.B.: / Ich habe bisher nichts von der App gehört / FreundInnen / Soziale Medien (Twitter, Facebook, YouTube, TikTok, etc.) / KollegInnen / Weiß ich nicht / Möchte ich nicht beantworten / Offizielle Corona-Warn-App Homepage

Wissen

- Q8 Welche Aussagen meinen Sie werden auf die App zutreffen? (Bitte kreuzen Sie alle an, die zutreffen.)
  - Die App benutzt Bluetooth.
  - Die App stellt fest, welche anderen Smartphones, die auch die App nutzen, in der Nähe sind.
  - Die Nutzung der App wird verpflichtend.
  - Die App benutzt Ortungsdienste (wie GPS).

  - Die App ermöglicht es mir, Gesundheitsdaten für Forschungszwecke an das Robert Koch-Institut zu spenden.
  - Die App kann genutzt werden, um anderen zu zeigen, dass ich aktuell nicht mit COVID-19 infiziert bin.
  - Die App ermöglicht es der Regierung zu sehen, wo ich mich aktuell befinde.
  - Die App bedroht meine Privatsphäre.
  - Die App schränkt meine Grundrechte ein.
  - Die App kann helfen die Verbreitung des COVID-19 Virus zu bekämpfen.
  - Die App teilt Namen und Telefonnummern meiner Kontakte mit der Regierung.
  - Die App ermöglicht es der Regierung zu sehen, wenn Menschen den Sicherheitsabstand zu Anderen nicht einhalten.
  - Die App teilt temporäre IDs und Zeitstempel.
  - Die App teilt Fitnessdaten.
  - Die App teilt ein Bewegungsprofil von mir.
  - Die App hilft zu entscheiden, wer auf COVID-19 getestet werden sollte.
  - Keine der genannten Eigenschaften.
  - Weiß ich nicht

- Q9 Welche Aussagen glauben Sie treffen auf die App zu, wenn andere NutzerInnen sich mit COVID-19 infiziert haben? (Bitte kreuzen Sie alle an, die zutreffen.)
  - Die App informiert mich, wenn eine infizierte Person in der Nähe ist.
  - Die App informiert mich im Nachhinein, wenn ich mit einer Person Kontakt hatte, die später positiv auf COVID-19 getestet wurde.
  - Die App ermöglicht es der Regierung zu sehen, wenn jemand sich nicht an eine verordnete Quarantäne hält.
  - Keine der genannten Eigenschaften.
  - Weiß ich nicht.

- Q10 Welche Aussagen glauben Sie treffen auf die App zu, wenn Sie selbst positiv auf COVID-19 getestet wurden? (Bitte kreuzen Sie alle an, die zutreffen.)
  - Die App informiert andere NutzerInnen der App, die in meiner Nähe waren, dass sie sich vielleicht angesteckt haben.
  - Ein Arzt / Eine Ärztin oder das Gesundheitsamt muss meinen positiven COVID-19 Test bestätigen, bevor die Daten aus der App an das RKI geschickt werden.
  - Die Daten aus der App werden kontinuierlich an das RKI geschickt.
  - Die App ermöglicht es der Regierung zu sehen, wenn ich mich nicht an eine verordnete Quarantäne halte.
  - Keine der genannten Eigenschaften.
  - Weiß ich nicht.

App Beschreibung und Verständnis

Im Folgenden geben wir eine kurze Einführung über die geplanten Fähigkeiten der Contact-Tracing App.
Die Bundesregierung plant, in naher Zukunft eine App für Smartphones zur Nachverfolgung der Ansteckungen mit COVID-19 einzuführen. Die Nutzung der App soll freiwillig und sehr einfach sein. Die App soll dabei helfen Infektionen früher zu erkennen. Damit können gezielte Maßnahmen zur Eindämmung ermöglicht werden.
Wenn Sie die App benutzen, würde die App feststellen, welche anderen NutzerInnen der App in Ihrer Nähe sind. Hierfür würde die App Bluetooth nutzen. Die App kann Sie dann darüber informieren, falls Sie sich in den letzten Tagen in der Nähe einer Person befunden haben, die später positiv auf COVID-19 getestet wurde. Die App würde Sie dann darüber informieren wie Sie sich verhalten sollen, z.B. sich auf COVID-19 testen zu lassen.

- Q11 Was wird die beschriebene App nutzen, um festzustellen wer sich in der Nähe aufgehalten hat?
  [Bluetooth / Ortungsdienste (wie GPS) / Kontakte aus meinem Telefonbuch / Weiß ich nicht]

Installation der App

Stellen Sie sich für die folgenden Fragen bitte vor, dass die zuvor beschriebene App bereits existiert. Die App wird von SAP entwickelt und die Infrastruktur wird von der Deutschen Telekom betrieben. Das Robert Koch-Institut (RKI) ist für die App verantwortlich und wertet die Daten aus. Die Daten dürfen nur für die Bekämpfung von COVID-19 genutzt werden.

- Q12 Mit welcher Wahrscheinlichkeit würden Sie die App nutzen?
  [Auf jeden Fall nutzen / Wahrscheinlich nutzen / Ich bin unentschieden / Wahrscheinlich nicht nutzen / Auf keinen Fall nutzen / Möchte ich nicht sagen / Weiß ich nicht]
- Q13 Was ist der Hauptgrund für Ihre Antwort?
  [Freitext]

Mögliche Eigenschaften

Q14 Im Folgenden werden wir Ihnen 24 Aussagen präsentieren. Diese Aussagen sind Eigenschaften, die die App haben **könnte**. Bitte wählen Sie aus, wie diese Aussagen, **wenn sie zutreffen würden**, Ihre Bereitschaft die App zu nutzen beeinflussen würden.
[Auf jeden Fall nutzen / Eher nutzen / Kein Einfluss / Eher nicht nutzen / Auf keinen Fall nutzen / Weiß ich nicht]

- Die App würde mich benachrichtigen, falls ich einem COVID-19 Ansteckungsrisiko ausgesetzt war.
- Falls ich positiv auf COVID-19 getestet werde, würde die App automatisch andere NutzerInnen der App benachrichtigen, die sich bei mir anstecken konnten.
- Die App würde Menschen über Ansteckungsrisiken informieren, die darüber sonst nicht vom Gesundheitsamt informiert werden würden.
- Die App würde dem RKI helfen die COVID-19 Lage in Deutschland besser einzuschätzen.
- Die Nutzung der App würde es der Bevölkerung ermöglichen schneller zum öffentlichen Leben zurückzukehren.
- Die Nutzung der App würde es ermöglichen, die Wirtschaft schneller wieder hochzufahren.

- Falls ich positiv auf COVID-19 getestet werde, würde die App es dem RKI ermöglichen zu sehen mit wem ich Kontakt hatte, um diese Personen zu informieren.
- Falls jemand in meinem Umfeld positiv auf COVID-19 getestet wird, würde die App es dem RKI ermöglichen zu sehen, dass ich mit dieser Person Kontakt hatte, um mich zu informieren.
- Falls ich positiv auf COVID-19 getestet werde, könnten Hacker in meiner Umgebung rausfinden, dass ich infiziert bin.
- Die Nutzung der App würde es dem RKI ermöglichen zu erfahren, wenn ich den Mindestabstand zu anderen Personen nicht einhalte.
- Die App würde Informationen über meinen Aufenthaltsort nutzen, um das Infektionsrisiko für andere besser einzuschätzen.
- Es bestünde die Möglichkeit, dass die App fälschlicherweise ein Ansteckungsrisiko meldet und ich mich deshalb unnötig in Quarantäne begeben muss.
- Es bestünde die Möglichkeit, dass die App fälschlicherweise ein Ansteckungsrisiko meldet und ich mich deshalb unnötig testen lasse.
- Falls mich die App über ein Ansteckungsrisiko informiert, müsste ich mich in gesetzlich verordnete Quarantäne begeben.
- Das RKI hätte eine Datenbank mit Kontaktinformationen von Infizierten und von Personen mit denen diese Kontakt hatten.
- Der Schutz der Daten würde durch ein für die App entworfenes, neues Gesetz gewährleistet.
- Der Schutz der Daten würde durch eine Datenschutzerklärung und die Datenschutzgrundverordnung gewährleistet.
- Der Schutz der Daten würde durch technische Maßnahmen gewährleistet.
- Die App würde vom deutschen Bundesamt für Sicherheit in der Informationstechnik (BSI) auf Datensicherheit und Datenschutz überprüft.
- Die App würde von unabhängigen SicherheitsexpertInnen auf Datensicherheit und Datenschutz überprüft.
- Die App würde keine Informationen über meinen Aufenthaltsort erheben.
- Dies ist eine Aufmerksamkeitsfrage. Bitte wählen Sie als Antwort "Kein Einfluss" aus.
- Die App wäre Open Source.
- Der Staat würde durch Gesetze, aber nicht durch technische Maßnahmen daran gehindert, die Daten für Überwachung zu missbrauchen.

Es wird diskutiert, ob die App eine Voraussetzung für die Nutzung verschiedener Einrichtungen sein sollte, z.B. Restaurants, Bus und Bahn, etc.

Da in solchen Einrichtungen viele Menschen zusammenkommen, wäre eine gezielte Ermittlung von Infektionsrisiken hilfreich. Bedenken Sie dabei jedoch bitte, dass ca. 20% der Bevölkerung in Deutschland kein Smartphone besitzt und somit diese Einrichtungen nicht mehr nutzen könnte.

- Q15 Würden Sie diese Art Nutzungsvoraussetzung befürworten oder ablehnen?
  [Voll befürworten / Eher befürworten / Weder befürworten noch ablehnen / Eher ablehnen / Voll ablehnen / Möchte ich nicht sagen / Weiß ich nicht]

Demographische Daten

- Q16 Was ist Ihr Geschlecht?
  [Männlich / Weiblich / Nicht binär / Möchte ich selbst beschreiben: / Möchte ich nicht sagen]
- Q17 Was ist Ihr beruflicher Status?
  [SchülerIn / StudentIn / Angestellt / Beamter / Selbstständig / Freiberuflich / Arbeitssuchend / RentnerIn / Möchte ich nicht sagen]
- Q18 Haben Sie spezielle Computerfähigkeiten wie: System-Administration, Programmieren, IT-Sicherheit, Tech-support, Power-User etc.
  [Ja / Nein / Möchte ich nicht sagen]
- Q19 Inwieweit stimmen Sie der folgenden Aussage zu oder lehnen sie ab: "In der Regel vertraue ich darauf, dass die Regierung das Richtige tut."
  [Stimme vollständig zu / Stimme eher zu / Stimme weder zu, noch lehne ab / Lehne eher ab / Lehne vollständig ab / Möchte ich nicht sagen]
- Q20 Welcher Partei stehen Sie am nächsten?
  [Grüne / CDU/CSU / SPD / FDP / AfD / Die Linke / Andere/Möchte ich nicht sagen]
- Q21 Wie häufig haben Sie derzeit in Person engen Kontakt zu Menschen außerhalb Ihres Haushaltes?
  [Höchstens einmal pro Woche / Ein paar Mal pro Woche / Ein paar Mal pro Tag / Viele Male pro Tag / Möchte ich nicht sagen]
- Q22 Wie besorgt bzw. unbesorgt sind Sie wegen COVID-19 in den folgenden drei Bereichen?
  Gesundheit, Wirtschaft, Soziales
  [Unbesorgt / Ein wenig besorgt / Besorgt / Sehr besorgt / Möchte ich nicht sagen]
- Q23 Gehören Sie zu einer COVID-19 Risikogruppe?
  [Ja / Nein / Weiß ich nicht / Möchte ich nicht sagen]
- Q24 Gehört eine Ihnen nahestehende Person zu einer COVID-19 Risikogruppe?
  [Ja / Nein / Weiß ich nicht / Möchte ich nicht sagen]
- Q25 Sind Sie oder ist jemand in Ihrem persönlichen Umfeld bereits an Covid-19 erkrankt?
  [Ja / Nein / Weiß ich nicht / Möchte ich nicht sagen]
- Q26 Ist in Ihrem persönlichen Umfeld bereits jemand an Covid-19 verstorben?
  [Ja / Nein / Weiß ich nicht / Möchte ich nicht sagen]
- Q27 Wie wirkt sich die Covid-19 Pandemie auf Ihre finanzielle Situation aus?
  [Positiv / Gar nicht / Negativ / Wirtschaftliche Existenz ist bedroht / Möchte ich nicht sagen]
- Q28 Müssen Sie jemanden wegen der Covid-19 Pandemie zuhause betreuen?
  [Ja / Nein / Möchte ich nicht sagen]
- Q29 Wie hat sich die Krise auf Ihre Arbeit ausgewirkt?
  [Gar nicht / Home Office / Kurzarbeit / Job verloren / Job gefunden / Möchte ich nicht sagen]

Danke!

Wenn Sie mehr über das Coronavirus erfahren und herausfinden möchten, wie Sie sich und Ihre Familie bestmöglich schützen können, klicken Sie auf diesen Link zur Coronavirus-Website der Bundeszentrale für gesundheitliche Aufklärung: https://www.infektionsschutz.de/coronavirus/
Vielen Dank dass Sie an unserer Studie teilgenommen haben!
Wenn Sie Feedback haben oder noch Ihre Meinung zu der App mitteilen wollen, können Sie das in dem untenstehenden Feld tun. Alternativ können Sie sich auch direkt an die Forscher wenden, indem Sie eine Mail an study@lists.iai.uni-bonn.de senden.

A.2 Additional Tables and Figures

Factor	Description	Baseline
Required		
Trust in Government	5-point scale. Fully trust to fully distrust towards the government.	Neither
Optional		
Beliefs	3 multi-choice questions. Beliefs about the app in general, personal context, and related to others.	n/a
Worries	3 questions; 4-point scales. How worried are participants regarding future health, economy, and social life.	Not worried
Media Sources	Multi-choice question. From which media sources participants learned about the app.	n/a
Personal	6 questions; Yes, No & "Don't know". Health risks, previous infection, deaths, and other personal effects.	No
Demographics	7 questions. General demographic questions such as tech background, age, gender, and job.	various

TABLE A.1: Factor categories appearing in the candidate regression models. Model candidates always included the required factors and covered all possible combinations of optional factors. Final models were selected based on lowest AIC. Categorical factors are individually compared to their listed baseline.

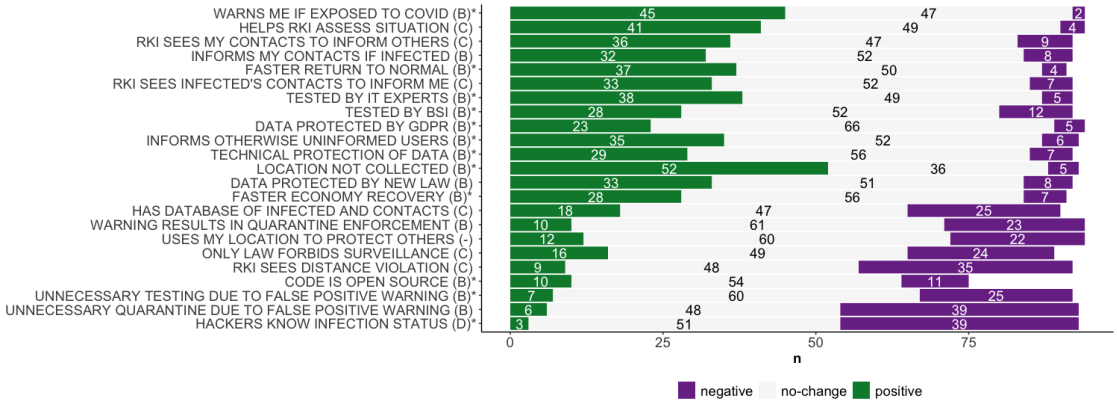


FIGURE A.1: The figure shows whether potential properties would change their mind for participants who ticked that they would probably not install the app.

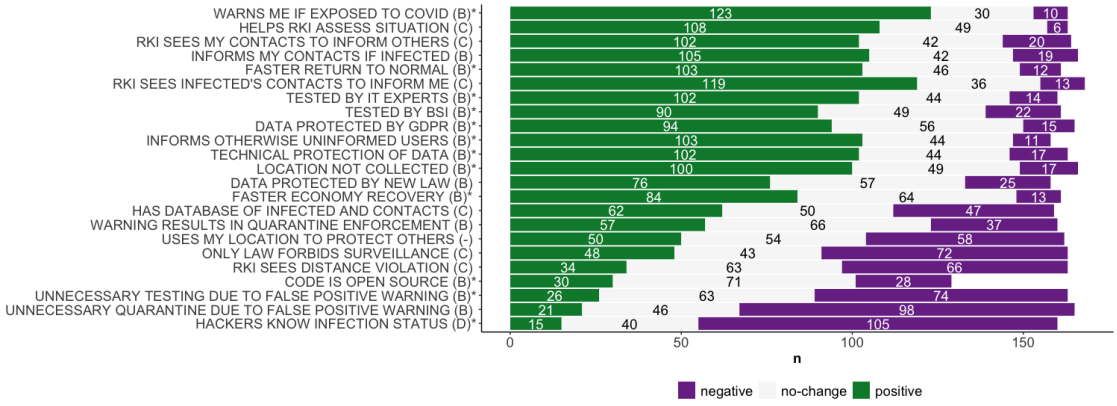


FIGURE A.2: The figure shows whether potential properties would change their mind for participants who ticked that they were neutral about the intention to install the app.

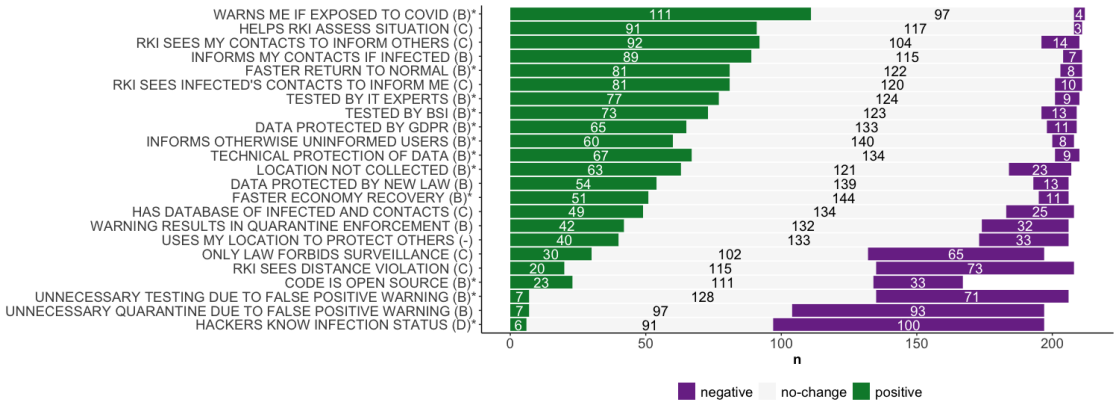


FIGURE A.3: The figure shows whether potential properties would change their mind for participants who ticked that they would probably install the app.

Abbreviation	Question	True?
General attributes		
(GEN) SHARES MOTION PROFILE	The app shares a profile of my movement.	✗[206]
(GEN) SHARES TEMPORARY IDS	The app shares temporary IDs and timestamps.	✓[215]
(GEN) SHARE PHONE CONTACTS WITH GOVERNMENT	The app shares the names and phone numbers of my contacts with the government.	✗[68]
(GEN) GOVERNMENT CAN TRACK ME	The app enables the government to see my current location.	✗[206]
(GEN) THREATS PRIVACY	The app undermines my privacy.	-
(GEN) DETECTS NEARBY USERS	The app determines when other smartphones are nearby that are also using the app.	✓[215]
(GEN) HELPS WITH TESTING DECISION	The app facilitates decision-making on who should be tested for COVID-19.	✓[75]
(GEN) SHARES FITNESS DATA	The app shares fitness data.	✗[44]
(GEN) SHOWS NEGATIVE INFECTION STATE	The app can be used to demonstrate to others that I am not currently COVID-19 positive.	✗
(GEN) FIGHTS DISEASE SPREAD	The app can help fight the spread of the COVID-19 virus.	✓[215]
(GEN) CAN DONATE HEALTH DATA	Through the app I can donate health data to the RKI for research purposes.	✗[44]
(GEN) RESTRICTS BASIC RIGHTS	The app infringes my fundamental rights.	-
(GEN) GOVERNMENT SEES DISTANCE VIOLATION	The app enables the government to see if people are not keeping a safe distance from others.	✗[52]
(GEN) USES LOCATION SERVICES	The app uses location services (like GPS).	- [52, 20]
(GEN) MANDATORY USAGE	Usage of the app will be mandatory.	✗[215]
(GEN) USES BLUETOOTH	The app uses Bluetooth.	✓[215]
(GEN) NONE	None of the above applies	✗
Attributes if others are infected		
(OTH) INFORMS IF INFECTED NEARBY	The app notifies me when an infected person is located nearby.	✗[52]
(OTH) INFORMS IF CONTACTED INFECTED	The app notifies me if I have had contact with an individual who later tested positive for COVID-19.	✓[215]
(OTH) GOVERNMENT SEES QUARANTINE VIOLATION	The app enables the government to see if someone is not complying with quarantine orders.	✗[52]
(OTH) NONE	None of the above applies	✗
Attributes if I myself am infected		
(SLF) DATA TRANSMISSION ONLY AFTER CONFIRMATION	A physician or the public health authority has to confirm my positive COVID-19 test result before the app sends data to the RKI.	✓[52]
(SLF) INFORMS MY CONTACTS	The app informs other app users who have been close to me that they may have contracted the virus.	✓[215]
(SLF) GOVERNMENT SEES QUARANTINE VIOLATION	The app enables the government to see if I am not complying with quarantine orders.	✗[52]
(SLF) SHARES DATA CONTINUOUSLY	The app sends data continuously to the RKI.	✗[52]
(SLF) NONE	None of the above applies	✗

TABLE A.2: Overview of all statements the participants were presented with and for which they had to decide whether they apply to the to be released CWA. The last column indicates if the attribute is correct for the app.

Abbreviation (Potential Property)	Full statement	True?	Approach (Central/ Decentral/Both)
(PP) ONLY LAW PREVENTS SURVEILLANCE	The government would be prevented by law, but not by technical means, from misusing the data for surveillance purposes.	✗[166]	C
(PP) TECHNICAL PROTECTION OF DATA	Technical measures would be implemented to ensure the data are protected.	✓[166]	B
(PP) RKI SEES INFECTED'S CONTACTS TO INFORM ME	If somebody near me has tested positive for COVID-19, the app would enable the RKI to see that I have had contact with that individual in order to notify me accordingly.	✗[166]	C
(PP) RKI SEES MY CONTACTS TO INFORM OTHERS	If I test positive for COVID-19, the app would allow the RKI to see who I had contact with in order to notify those individuals.	✗[166]	C
(PP) RKI SEES DISTANCE VIOLATION	Using the app would enable the RKI to find out if I am not complying with minimum distancing to other individuals.	✗[166]	C
(PP) HAS DATABASE OF INFECTED AND CONTACTS	The RKI would have a database with the contact data of infected individuals and the people they have had contact with.	✗[166]	C
(PP) HELPS RKI ASSESS SITUATION	The app would support the RKI to better assess the COVID-19 situation.	✗	C
(PP) USES MY LOCATION TO PROTECT OTHERS	The app would use information about my location to more accurately monitor infection risk for others.	✗[52]	-
(PP) LOCATION NOT COLLECTED	The app would not collect any data about my location.	✓[52]	B
(PP) TESTED BY BSI	The German Federal Office for Information Security(BSI) would verify that the app fulfills data security and data protection requirements.	✓[26]	B
(PP) FASTER RETURN TO NORMAL	Using the app would make possible a speedier return to normal public life.	✓[107]	B
(PP) UNNECESSARY QUARANTINE DUE TO FALSE POSITIVE WARNING	There is a possibility that the app could incorrectly report infection risk, resulting in me having to quarantine unnecessarily.	✗[51]	B
(PP) FASTER ECONOMY RECOVERY	Using the app would help restart the economy faster.	✓	B
(PP) WARNING RESULTS IN QUARANTINE ENFORCEMENT	If the app notifies me that I may have been infected, I would have be required by law to quarantine.	✗[51]	B
(PP) WARNS ME IF EXPOSED TO COVID	The app would notify me if I have been in a situation putting me at risk of contracting COVID-19.	✓[215]	B
(PP) UNNECESSARY TESTING DUE TO FALSE POSITIVE WARNING	There is a possibility that the app could incorrectly report infection risk, resulting in me having to get tested unnecessarily.	✓[75]	B
(PP) TESTED BY IT EXPERTS	Independent security experts would verify that the app fulfills data security and data protection requirements.	✓[1]	B
(PP) DATA PROTECTED BY GDPR	Protection of the data would be guaranteed pursuant to a data protection policy and the General Data Protection Regulation.	✓[166]	B
(PP) INFORMS OTHERWISE UNINFORMED USERS	The app would inform people of infection risk who would not otherwise be contacted by the public health authority.	✓[215]	B
(PP) HACKERS KNOW INFECTION STATUS	Any nearby hackers could find out if I have tested positive for COVID-19.	✓[16]	D
(PP) DATA PROTECTED BY NEW LAW	Protection of the data would be guaranteed under a new law drafted especially for the app.	✗	B
(PP) INFORMS MY CONTACTS IF INFECTED	If I have tested positive for COVID-19, the app would automatically notify other users of the app who are at risk being exposed through contact with me.	✗[166]	B
(PP) CODE IS OPEN SOURCE	The app would be open-source	✓[53]	B

TABLE A.3: The presented potential properties are either true for the centralized (C) or the decentralized (D) approach, or true for both (B) app designs. The properties that did not depend on the design approach is marked with "-".

Currently, how frequently do you have close personal contact with people not from your household?					
Once a week at most	39.5	A few times a week	37.8	A few times a day	10.2
Several times a day	10.1	Not disclosed	2.4		
How concerned or unconcerned are you about COVID-19 in regard to the following three areas?					
Health					
Unconcerned	16.0	A bit concerned	39.4	Concerned	25.7
Very concerned	18.3	Not disclosed	0.7		
The economy					
Unconcerned	7.3	A bit concerned	22.5	Concerned	34.5
Very concerned	35.2	Not disclosed	0.5		
Society					
Unconcerned	11.3	A bit concerned	23.9	Concerned	35.8
Very concerned	28.1	Not disclosed	0.9		
Do you fall within a COVID-19 high-risk group?					
Yes	31.1	No	58.1	Don't know	9.8
Not disclosed	1.9				
Does someone close to you fall within a COVID-19 high-risk group?					
Yes	62.2	No	31.3	Don't know	5.8
Not disclosed	0.7				
Have you or any person close to you fallen ill with Covid-19?					
Yes	7.5	No	86.8	Don't know	5.0
Not disclosed	0.7				
Has anyone close to you died of Covid-19?					
Yes	3.0	No	94.9	Don't know	1.8
Not disclosed	0.4				
How has the Covid-19 pandemic affected you financially?					
Positive impact	3.2	No impact	58.9	Negative impact	32.4
Critical impact	3.2	Not disclosed	2.3		
Has the Covid-19 pandemic resulted in you having to look after/care for someone at home?					
Yes	9.4	No	89.9	Not disclosed	0.7
How has the crisis affected your work?					
Unaffected	52.7	Working from home	24.5	Short-time work	13.6
Became unemployed	5.0	Found employment	0.9	Not disclosed	3.4

TABLE A.4: Impact of the Covid-19 pandemic on participants. Numbers report the percentages in each question ($n = 744$).

Potential Property	Def-No and Prob-No	Def-No and Undecided	Def-No and Prob-Yes	Def-No and Def-Yes	Prob-No and Undecided	Prob-No and Prob-Yes	Prob-No and Def-Yes	Undecided and Prob-Yes	Undecided and Def-Yes	Prob-Yes and Def-Yes
(PP) WARNS ME IF EXPOSED TO COVID	**0.42**	**0.55**	**0.68**	**0.81**	**0.27**	**0.54**	**0.76**	**0.37**	**0.62**	**0.34**
(PP) INFORMS MY CONTACTS IF INFECTED	**0.37**	**0.55**	**0.67**	**0.81**	**0.32**	**0.56**	**0.75**	**0.33**	**0.59**	**0.33**
(PP) INFORMS OTHERWISE UNINFORMED USERS	**0.43**	**0.58**	**0.66**	**0.77**	**0.23**	**0.42**	**0.62**	**0.25**	**0.51**	**0.34**
(PP) HELPS RKI ASSESS SITUATION	**0.48**	**0.61**	**0.71**	**0.85**	**0.25**	**0.51**	**0.76**	**0.33**	**0.63**	**0.38**
(PP) FASTER RETURN TO NORMAL	**0.37**	**0.49**	**0.63**	**0.77**	**0.22**	**0.47**	**0.68**	**0.3**	**0.55**	**0.33**
(PP) FASTER ECONOMY RECOVERY	**0.29**	**0.45**	**0.53**	**0.66**	**0.23**	**0.37**	**0.54**	**0.19**	**0.41**	**0.25**
(PP) RKI SEES MY CONTACTS TO INFORM OTHERS	**0.39**	**0.55**	**0.64**	**0.79**	**0.24**	**0.45**	**0.7**	**0.3**	**0.6**	**0.34**
(PP) RKI SEES INFECTED'S CONTACTS TO INFORM ME	**0.39**	**0.59**	**0.67**	**0.8**	**0.35**	**0.51**	**0.71**	**0.26**	**0.55**	**0.34**
(PP) HACKERS KNOW INFECTION STATUS	**0.31**	**0.35**	**0.46**	**0.58**	0.06	**0.19**	**0.36**	**0.15**	**0.31**	**0.19**
(PP) RKI SEES DISTANCE VIOLATION	**0.24**	**0.42**	**0.49**	**0.61**	**0.22**	**0.31**	**0.47**	0.12	**0.32**	**0.22**
(PP) USES MY LOCATION TO PROTECT OTHERS	**0.36**	**0.5**	**0.64**	**0.75**	**0.22**	**0.49**	**0.66**	**0.34**	**0.56**	**0.31**
(PP) UNNECESSARY QUARANTINE DUE TO FALSE POSITIVE WARNING	**0.29**	**0.44**	**0.52**	**0.63**	0.17	**0.28**	**0.43**	**0.15**	**0.33**	**0.2**
(PP) UNNECESSARY TESTING DUE TO FALSE POSITIVE WARNING	**0.32**	**0.46**	**0.51**	**0.67**	**0.18**	**0.27**	**0.5**	0.11	**0.38**	**0.3**
(PP) WARNING RESULTS IN QUARANTINE ENFORCEMENT	**0.26**	**0.53**	**0.59**	**0.74**	**0.36**	**0.49**	**0.67**	**0.23**	**0.5**	**0.31**
(PP) HAS DATABASE OF INFECTED AND CONTACTS	**0.25**	**0.48**	**0.6**	**0.72**	**0.27**	**0.48**	**0.63**	**0.31**	**0.51**	**0.27**
(PP) DATA PROTECTED BY NEW LAW	**0.4**	**0.49**	**0.61**	**0.74**	0.14	**0.41**	**0.62**	**0.29**	**0.53**	**0.31**
(PP) DATA PROTECTED BY GDPR	**0.38**	**0.56**	**0.65**	**0.79**	**0.31**	**0.5**	**0.71**	**0.28**	**0.57**	**0.36**
(PP) TECHNICAL PROTECTION OF DATA	**0.35**	**0.51**	**0.63**	**0.76**	**0.27**	**0.48**	**0.68**	**0.3**	**0.57**	**0.34**
(PP) TESTED BY BSI	**0.32**	**0.49**	**0.64**	**0.79**	**0.24**	**0.48**	**0.7**	**0.31**	**0.57**	**0.33**
(PP) TESTED BY IT EXPERTS	**0.38**	**0.52**	**0.63**	**0.76**	**0.23**	**0.45**	**0.66**	**0.28**	**0.52**	**0.3**
(PP) LOCATION NOT COLLECTED	**0.35**	**0.38**	**0.42**	**0.61**	0.06	0.16	**0.44**	0.11	**0.4**	**0.28**
(PP) CODE IS OPEN SOURCE	**0.36**	**0.44**	**0.46**	**0.53**	0.12	**0.2**	**0.32**	0.1	**0.24**	**0.15**
(PP) ONLY LAW PREVENTS SURVEILLANCE	**0.32**	**0.39**	**0.48**	**0.64**	0.09	**0.22**	**0.45**	0.14	**0.38**	**0.26**

TABLE A.5: Effect sizes of comparison between the general installation intention groups. Bright grey indicate a small effect (0.10 - < 0.3), darker grey a moderate effect (0.30 - < 0.5) and the darkest grey a large effect (>= 0.5).

Appendix B

Appendix for "Less About Privacy"

B.1 Study Material

Survey

Screening Questions

- Q1 What is your age?
  [Free Text]
- Q2 In which federal state do you live?
  [List of all German federal states / I don't want to state]
- Q3 Do you use a smartphone?
  [Yes, an Android / Yes, an iPhone / Yes, another smartphone / Yes, but I don't know which / No / I don't want to state]
- Q4 What is your netto household income?
  [<= 1300€ / 1300-1700€ / 1700-2600€ / 2600-3600€ / 3600-5000€ / >5000€ / I don't want to state]
- Q5 What is the number of individuals living in your household?
  [1 / 2 / 3 / 4 or more / I don't want to state]
- Q6 What is the highest-level vocational qualification you hold?
  [Completed apprenticeship / Other; Vocational qualification: / University degree / Master or Technician certification or equivalent technical school diploma / Vocational school diploma / Technical school diploma / No vocational qualification / Technical college degree (or engineering school diploma) / I don't want to state / Abitur (German university entrance qualification)]

App Description and Media Sources The COVID-19 coronavirus pandemic is a worldwide problem. The Corona-warn-app for Germany is one of the measures to assist health authorities in tracing and containing infection. The app was developed by SAP. It runs on Deutsche Telekom infrastructure. The App was published by the Robert Koch Institute (RKI). It has also been referred to as the 'Corona app', 'COVID app' or 'contact tracing app' in the past.

- Q7 Have you heard of the app? If 'yes', please select where you heard about the app. Multiple selections possible.
  [Public broadcasters (ARD, ZDF, WDR, etc.) / Non-public TV (Pro7, Vox, N24, etc.) / Scientific publications / Newspapers, journals, magazines, etc. / Family member / Official government/state agency websites (Robert Koch Institute, Federal Government, etc.) / Other websites: / I have not heard about this app / Friends / Social media (Twitter, Facebook, YouTube, TikTok, etc.) / Work colleagues/associates / Don't know/I don't want to state / Official Corona Warning App website]

Knowledge

- Q8 Which of the below statements do you think apply regarding the app? (please check **all** that apply.)
  (Short identifier for paper, True?, `B` if basic functionality included in [165])
  - The app uses Bluetooth. (`USES BLUETOOTH`, ✓, `B`)
  - Through the app I can donate health data to the Robert Koch Institute for research purposes. (`CAN DONATE HEALTH DATA`, ×)
  - The app determines when other smartphones are nearby that are also using the app. (`DETECTS NEARBY USERS`, ✓, `B`)
  - The app shares temporary IDs and timestamps. (`SHARES TEMPORARY IDS`, ✓, `B`)
  - The app enables the government to see my current location. (`GOVERNMENT CAN TRACK ME`, ×)
  - The app enables the government to see if people are not keeping a safe distance from others. (`GOVERNMENT SEES DISTANCE VIOLATION`, ×)
  - Usage of the app is mandatory. (`MANDATORY USAGE`, ×)
  - The app shares the names and phone numbers of my contacts with the government. (`SHARE PHONE CONTACTS WITH GOVERNMENT`, ×)
  - The app infringes my basic rights. (`RESTRICTS BASIC RIGHTS`, -)
  - The app can be used to demonstrate to others that I am not currently COVID-19 positive. (`SHOWS NEGATIVE INFECTION STATE`, ×)
  - The app facilitates decision-making on who should be tested for COVID-19. (`HELPS WITH TESTING DECISION`, -)
  - The app shares fitness data. (`SHARES FITNESS DATA`, ×)
  - The app can help fight the spread of the COVID-19 virus. (`FIGHTS DISEASE SPREAD`, -)
  - The app uses location services (like GPS). (`USES LOCATION SERVICES`, -)
  - The app shares a profile of my movement. (`SHARES MOTION PROFILE`, ×)

  - The app undermines my privacy. (THREATS PRIVACY, -)
  - None of the above applies.(NONE (GENERAL), ×)
  - Don't know

- Q9 What statements do you think apply regarding the app when other users are COVID-19 positive? (please check **all** that apply.)
  - The app enables the government to see if someone is not complying with quarantine orders. (GOVERNMENT SEES OTHERS' QUARANTINE VIOLATION, ×)
  - The app notifies me if I have had contact with an individual who later tested positive for COVID-19. (INFORMS ME IF CONTACT INFECTED, ✓, B)
  - The app notifies me when an infected person is located nearby. (INFORMS IF INFECTED NEARBY, ×)
  - None of the above applies. (NONE (OTHER), ×)
  - Don't know

- Q10 What statements do you think apply regarding the app when you yourself are COVID-19 positive? (please check **all** that apply.)
  - The app informs other app users who have been close to me that they may have contracted the virus. (INFORMS MY CONTACTS, ✓, B)
  - The app sends data continuously to the RKI. (SHARES DATA CONTINUOUSLY, ×)
  - A physician or the public health authority has to confirm my positive COVID-19 test result before the app sends data to the RKI. (DATA TRANSMISSION ONLY AFTER CONFIRMATION, ✓)
  - The app enables the government to see if I am not complying with quarantine orders. (GOVERNMENT SEES MY QUARANTINE VIOLATION, ×)
  - None of the above applies. (NONE (SELF), ×)
  - Don't know

App Description and Comprehension A brief introduction is provided below on the capabilities of the contact-tracing app.
The federal government has introduced a smartphone app to trace COVID-19 transmission on June 16, 2020. The app is very user-friendly and its usage voluntary. The app is designed to ensure that virus transmission is detected more quickly. This allows taking targeted containment measures.
When in use, the app determines what other users of the app are located near you. The app does this via Bluetooth. The app will alert you if you have been near someone within the past few days who subsequently tested positive for COVID-19. The app then informs you of what you need to do next, such as get

tested for COVID-19.

- Q11 How will the described app determine what people have been near me?
  [Bluetooth / Wi-Fi / Location services (such as GPS) / My phone Contacts list / Don't know]

Install General The app was developed by SAP and runs on Deutsche Telekom infrastructure. The Robert Koch Institute (RKI) is in charge of the app and evaluates the data. The exclusive permissible usage of the data is to fight COVID-19.

- Q12 Do you have the corona-warn-app installed?
  [Yes / Yes, but uninstalled again / No / No, but I plan to install it / I don't want to state / Don't know]
- Q13 What is the primary reason for your answer?
  [Free text]

Previous Survey

- Q14 Did you participate in a very similar study in May or June?
  [Yes / No / Don't know / I don't want to state]

If Yes in Q14:

- Q15 In this survey you were ask if you would use the app. What did you answer back then?
  [I would use the app / I would NOT use the app / I can't remember what i answered / I guess I did not take part in this study after all / I don't want to state]

Depending on the participants' answer on Q12 and Q15:

- Q16a You stated at the time that you would use the app, but currently you do not have the app installed. Could you tell us what makes you not use the app?
  [Free text]
- Q16b You stated at the time that you would use the app, but currently you do not have the app installed. Could you tell us what makes you not use the app yet?
  [Free text]
- Q16c You stated at the time that you would not use the app, but currently you do have the app installed. Could you tell us what made you try the app after all?
  [Free text]

- Q16d You stated at the time that you would not use the app, currently you have the app installed then uninstalled again. Could you tell us what made you try the app after all?
  [Free text]

Reason to change opinion *Depending on the participants' answer on Q12:*

- Q17a *[If "Yes"]* You stated that you have installed the app. What new features or information would make you uninstall the app?
  [Free text]
- Q17b *[If "Yes, but uninstalled again"]* You stated that you have installed then uninstalled the app. What new features or information would make you use the app after all?
  [Free text]
- Q17c *[If "No"]* You stated that you have not installed the app. What new features or information would make you want to use the app?
  [Free text]

Potential Properties

- Q18 You will now be presented with 24 statements, some of which apply to the app, while others are not true. How do the statements affect your willingness to use the app? Please select **Not true** if you believe a statement does not apply to the current app.
  *[That's why I use the app / That's why I **don't** use the app / No influence / Not true / Don't know]*
  - The government is prevented by law, but not by technical means, from misusing the data for surveillance purposes.
  - Using the app enables the RKI to find out if I am not complying with minimum distancing to other individuals.
  - The RKI has a database with the contact data of infected individuals and the people they had contact with.
  - If I test positive for COVID-19, the app allow the RKI to see who I had contact with in order to notify those individuals.
  - The app has been reviewed by the German Federal Office for Information Security (BSI) for data security and data protection.
  - Using the app makes a speedier return to normal public life possible.
  - Technical measures were implemented to ensure the data is protected.
  - There is a possibility that the app could incorrectly report infection risk, resulting in me having to quarantine unnecessarily.
  - Using the app helps re-start the economy faster.

  - If the app notifies me that I may have been infected, I am required by law to quarantine.
  - The app notifies me if I have been in a situation putting me at risk of contracting COVID-19.
  - There is a possibility that the app could incorrectly report infection risk, resulting in me having to get tested unnecessarily.
  - The app has been reviewed by independent security experts for data security and data protection.
  - The app uses information about my location to monitor infection risk for others more accurately.
  - Protection of the data is guaranteed pursuant to a data protection policy and the General Data Protection Regulation (GDPR).
  - The app does not collect any data about my location.
  - The app informs people of infection risk who would not otherwise be contacted by the public health authority.
  - If I have tested positive for COVID-19, any nearby hackers could find out I have tested positive.
  - This question pertains to attentive completion of the survey. Please select "No influence" as response.
  - If I have tested positive for COVID-19, the app automatically notifies other users of the app who are at risk of being exposed through contact with me.
  - The app is open-source.
  - The app supports the RKI to better assess the COVID-19 situation.
  - Data protection is ensured by a new law designed for the app.
  - If somebody near me tests positive for COVID-19, the app enables the RKI to see that I have had contact with that individual in order to notify me accordingly.

It was discussed whether use of the app should be made mandatory to use certain facilities, e.g. restaurants, train, bus etc. Since many people congregate in such facilities, targeted identification of infection risks would be helpful. It must be considered however that roughly 20% of the German population would be excluded from using such services due to not having a smartphone.

- Q19 Would you approve or disapprove of such mandatory usage?
  [Approve entirely / Mainly approve / Neither approve nor disapprove / Mainly disapprove / Disapprove entirely / I don't want to state / Don't know]

Demographics

- Q20 What is your gender?
  [Male / Female / Non-binary / Would like to self-describe: / I don't want to state]

- Q21 What is your work status?
  [School student / University/college student / Employee / Civil servant / Self-employed / Freelancer / Unemployed / Retiree / I don't want to state]
- Q22 Do you have specialized computing skills, such as: system administration, programming, IT security, tech support, power user, etc?
  [Yes / No / I don't want to state]
- Q23 Please indicate your agreement or disagreement with the following: "I generally trust the government to do the right thing."
  [Fully agree / Mostly agree / Neither agree nor disagree / Mostly disagree / Fully disagree / I don't want to state]
- Q24 What party do you have the most affinity with?
  [The Greens / CDU/CSU / SPD / FDP / AfD / The Left / Others/I don't want to state]
- Q25 Currently, how frequently do you have close personal contact with people not from your household?
  [Once a week at most / A few times a week / A few times a day / Several times a day / I don't want to state]
- Q26 How concerned or unconcerned are you about COVID-19 in regard to the following three areas?
  Health, The economy, Society
  [Unconcerned / A bit concerned / Concerned / Very concerned / I don't want to state]
- Q27 Do you fall within a COVID-19 high-risk group?
  [Yes / No / Don't know / I don't want to state]
- Q28 Does someone close to you fall within a COVID-19 high-risk group?
  [Yes / No / Don't know / I don't want to state]
- Q29 Have you or any person close to you fallen ill with COVID-19?
  [Yes / No / Don't know / I don't want to state]
- Q30 Has anyone close to you died of COVID-19?
  [Yes / No / Don't know / I don't want to state]
- Q31 How has the COVID-19 pandemic affected you financially?
  [Positive impact / No impact / Negative impact / Critical impact / I don't want to state]
- Q32 Has the COVID-19 pandemic resulted in you having to look after/care for someone at home?
  [Yes / No / I don't want to state]
- Q33 How has the crisis affected your work?
  [Unaffected / Working from home / Short-time work / Became unemployed / Found employment / I don't want to state]

- Q34 Do you have an account at Facebook, Instagram, TikTok or Google? *[Yes / No / I don't want to state]*

B.2 Additional Tables and Figures

		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
Code	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
Code	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
Code	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
Code	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
Code	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
Code	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
Code	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
Code	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
Code	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**																				
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
Attributes	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
Attributes	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
Attributes	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
Attributes	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
Attributes	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
Attributes	**Incorrect attributes**																				
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
Attributes	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
Attributes	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
Attributes	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
Attributes	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
Attributes	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
Attributes	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
Attributes	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
Attributes	NONE (GENERAL)	0.3	0.5	0.7	-	-	-	-	1.0	0.5	0.4	-	0.6	-	-	-	-	0.3	0.4	0.4	0.7
Attributes	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
Attributes	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
Attributes	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
Attributes	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
Attributes	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
Attributes	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
Attributes	**No truth value assignable**																				
Attributes	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
Attributes	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
Attributes	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
Attributes	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
Attributes	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
Attributes	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
Attributes	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
Attributes	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 B.1: Table of occurred codes and marked attributes split by the socio-demographic groups "age" and "education". Numbers, except totals, in %.

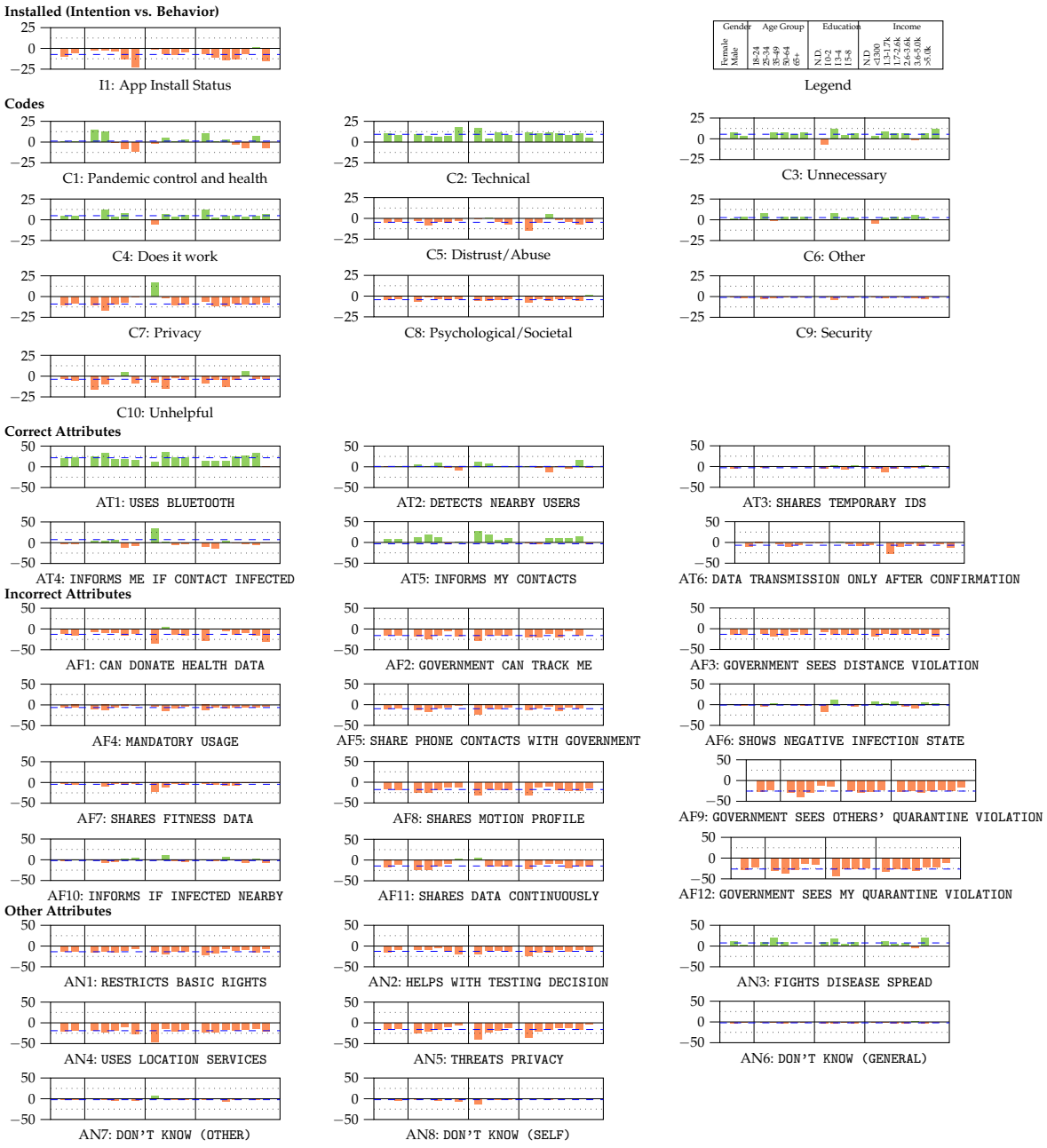


FIGURE B.1: Increase and decrease between percentage points of **app installation intention and action**, **high-level codes**, and knowledge **attributes** for different demographic groups. The blue dashed line represents the average of all groups. Order of socio-demographic groups: **Gender** (Female, Male); **Age** (18-24, 25-34, 35-49, 50-64, 65+); **Education** (Undefined/Not disclosed, ISCED 0-2, ISCED 3-4, ISCED 5-8); **Income** (Not disclosed, <= 1300€, 1300-1700€, 1700-2600€, 2600-3600€, 3600-5000€, >5000€)

		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
Code	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
Code	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
Code	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
Code	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
Code	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
Code	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
Code	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
Code	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
Code	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**
	Correct attributes																		
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
Attributes	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
Attributes	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
Attributes	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
Attributes	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
Attributes	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
Attributes	**Incorrect attributes**																		
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
Attributes	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
Attributes	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
Attributes	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
Attributes	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
Attributes	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
Attributes	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
Attributes	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
Attributes	NONE (GENERAL)	-	0.7	0.7	0.3	-	-	-	-	-	-	-	1.1	0.9	-	1.0	0.6	-	1.4
Attributes	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
Attributes	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
Attributes	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	-	-
Attributes	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
Attributes	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
Attributes	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
Attributes	**No truth value assignable**																		
Attributes	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
Attributes	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
Attributes	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
Attributes	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
Attributes	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
Attributes	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
Attributes	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
Attributes	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 B.2: Table of occurred codes and marked attributes split by the socio-demographic groups "gender" and "income". Numbers, except totals, in %.

Code	% in `cwa_beh`: (% ✓, % unclear, % ×)	ICR	Example
None	**46** (43.2, 56.8)	1	"None"
My Data/Technical	**25.7** (81.6, 18.4)		
Mission Creep/Data abuse/Privacy	**13.7** (93.0, 7.0)	1	"Disclosure of any data to anyone", "No misuse of personal data"
Surveillance	2.6 (94.7, 5.3)	0.91	"When I am under surveillance", "Being spied on less"
Changes of requirements	**7.1** (66.7, 33.3)	undef*	
GPS/Tracking	2.1 (80.0, 20.0)	1	"No location determination", "GPS tracking"
Contacts/Private Data	2.1 (100.0, 0.0)	1	"Access to my pictures, data, contact lists", "Registration by name"
Bluetooth	1.8 (0.0, 100.0)	1	"If it would work without bluetooth"
Generic different	0.5 (25.0, 75.0)	undef*	"If the way of collecting information should change radically compared to the current version"
Mobile Data/Internet	0.3 (50.0, 50.0)	undef*	"That it works without internet connection"
Generic more	0.3 (100.0, 0.0)	1	"if more data is stored that is not required for the purpose"
Security of data/Data protection	4.5 (66.7, 33.3)	1	"App gets hacked", "Legal changes in data protection"
Change from decentralized to centralized	0.4 (100.0, 0.0)	undef*	"When my data is no longer stored decentrally"
Functionality	**14.4** (32.4, 67.6)		
Malfunctions of App	**6.3** (41.3, 58.7)	1	"It should work properly", "Malfunctions"
More accurate measurement	0.3 (0.0, 100.0)	undef*	"Significantly shorten length of stay to infected"
Spreads (no) misinformation	0.8 (66.7, 33.3)	undef*	"If trivializes/favors the coronavirus", "it should provide better facts"
Compatibility (incl. new phone)	4.4 (0.0, 100.0)	1	"the app should work also on older models", "New smartphone"
Side effects	2.2 (56.2, 43.8)	undef*	"Less battery consumption", "High power or data consumption"
Additional Feature	1.5 (27.3, 72.7)	1	"Real time warning in case of proximity to infected persons", "Reminder function for fase mask, etc."
Usability better/worse	0.4 (33.3, 66.7)	undef*	"Easier usability/installation"
Advertisement	0.3 (100.0, 0.0)	undef*	"Just do not want to get additional advertising"
New and better app	0.3 (100.0, 0.0)	undef*	"If there was a better app"
No answer	**10.0** (41.1, 58.9)		
Don't know	7.8 (38.6, 61.4)	1	"Don't know"
Unclear	1.4 (60.0, 40.0)	1	"Who and when"
No answer	0.8 (33.3, 66.7)	1	"Don't want to state"
Political/Societal	**3.7** (15.4, 84.6)		
Expenses must be covered	1.1 (0.0, 100.0)	undef*	"When someone gives me a smartphone", "free mobile data", "If I get paid for it"
App mandatory	0.8 (0.0, 100.0)	undef*	"Only if it is mandatory"
Larger user base and correct usage	0.8 (0.0, 100.0)	undef*	"If more people had the app", "That all who tested positive immediately indicate this in the app"
App becomes chargeable/remains free of charge	0.4 (66.7, 33.3)	undef*	"Fees required"
General	0.3 (0.0, 100.0)	undef*	"Change of the entire government", "more testing is done"
Someone evaluates it as no longer necessary	0.3 (100.0, 0.0)	1	"The RKI no longer considers the APP necessary."
Help/Info	**3.5**(20.0, 80.0)		
Proof that app is useful/useless	1.4 (50.0, 50.0)	undef*	"That the app is useless", "Scientific evidence that this app makes a difference"
Info about security/data protection/functionality	1.0 (0.0, 100.0)	1	"More information about data protection", "Info whether Bluetooth is generally safe or not."
Others recommend it	0.4 (0.0, 100.0)	undef*	"there are positive reviews"
Assistance with installation	0.4 (0.0, 100.0)	1	"Assistance with the installation"
General	0.3 (0.0, 100.0)	undef*	"More precise info"
Pandemic development	**2.8** (76.2, 23.8)		
Pandemic's over	2.3 (94.1, 5.9)	1	"When Corona is over"
Increased infections	0.5 (0.0, 100.0)	1	"When infections increase in my city"
Personal	**1.3** (20.0, 80.0)		
Own situation changes	0.8 (0.0, 100.0)	1	"I'll install it as soon as I'm traveling more or have to go back to the office"
General	0.5 (50.0, 50.0)	undef*	"Since it's a company phone, I would first have to clarify if I'm allowed to install the app."
Additional codes	**0.6** (83.3, 16.6)		
Even X would be okay	0.5 (100.0, 0.0)	undef*	"even if my private data would be used I would have no problems with it"
Even X would not convince me	0.1 (0.0, 100.0)	undef*	"even if there would be a law I would rather go to [...] prison"

Table B.3: Full coding table for reasons to change opinion (Q17), 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.

Appendix C

Appendix for "I have not understood but agree"

C.1 Study Material

Survey Questionnaire

If a question concerns knowledge, the correct answer is indicated as ✗(if the statement does not apply to the app) or ✓(if the statement applies to the app). Please note that some topics are very complex, and covering edge cases and different understandings in a sentence proved to be hard. Therefore, we sometimes had to simplify the ratings. Those cases are marked with a * directly after the indication of whether a statement is correct or incorrect.

Demographics and installation status

1. Which gender do you identify most with?
   [randomized order, single-choice]
   (a) Male
   (b) Non-binary
   (c) Female
   (d) I would like to describe myself
   (e) Not specified
2. How old are you?
   [open-ended]
3. What is your highest level of education?
   [single-choice]
   (a) None
   (b) Hauptschulabschluss (High school diploma)
   (c) Realschulabschluss (High school diploma)

(d) A-level diploma
(e) Bachelor's degree
(f) Master's degree/diploma
(g) Apprenticeship
(h) Master craftsman
(i) Ph.D.
(j) Habilitation
(k) Other
(l) Not specified

4. Were you or are you active in the field of IT security, e.g., as a student, researcher, or practitioner?
[single-choice]

(a) No, never
(b) Yes, for less than 2 years
(c) Yes, between 2 and 5 years
(d) Yes, for more than 5 years

———————— Pagebreak ————————

The following part of this study is about the Corona-Warn-App. You will be asked questions, which we ask you to answer only in relation to the CWA (and not other apps such as the Luca app).

5. Have you heard about the CWA?
[single-choice]

(a) Yes
(b) No
(c) I am unsure

6. Have you installed the CWA on your smartphone?
[single-choice]

(a) Yes.
(b) I used to have, but no longer do.
(c) No, I never had either.
(d) No, the app cannot be installed on my smartphone.

(e) No, I do not have a smartphone.

(f) I do not know.

———————— Pagebreak ————————

Involved actors and data collection

Please indicate below to what extent you believe that the following statements are true.
Please only select "do not know" if you have no assumption at all to what extent a statement is true.

7. The following actors are involved in the creation of the CWA (e.g., as a developer, publisher, or client):
[randomized order, 7-point Likert scale, ranging from "fully agree" to "fully disagree" + " I do not know", single-choice for each item]

   (a) Governments outside the EU ✗*

   (b) German companies ✓

   (c) German government ✓

   (d) Robert Koch Institute (RKI) ✓

   (e) Companies outside the EU ✗*

   (f) Non-German companies within the EU ✗*

8. If you know of any other actors who are involved in the creation of the CWA, you can list them here:
[open-ended]

9. The CWA collects the following data for contact tracing and encounter notifications:

   (a) My location ✗

   (b) My IP address ✗

   (c) The information about how or when I use the app? ✗

   (d) My distance to others ✓

   (e) My demographic information (e.g., name, address) ✗

   (f) My cell phone model ✗

   (g) Random codes ✓

   (h) The duration of the encounter ✓

   (i) My infection status ✓

(j) The time of the encounter ✓

——————— Pagebreak ———————

10. The following actors have access to the "Location" data:
[randomized order, 7-point Likert scale, ranging from "fully agree" to "fully disagree" + " I do not know", single-choice for each item]:

    (a) The health departments ✗
    (b) Those involved in the development of the CWA ✗
    (c) The Robert Koch Institute ✗
    (d) Hackers ✗
    (e) The federal government ✗
    (f) Others: ✗

11. The following actors have access to the "Demographic information" data:
[randomized order, 7-point Likert scale, ranging from "fully agree" to "fully disagree" + " I do not know", single-choice for each item]:

    (a) The health departments ✗
    (b) Those involved in the development of the CWA ✗
    (c) The Robert Koch Institute ✗
    (d) Hackers ✗
    (e) The federal government ✗
    (f) Others: ✗

——————— Pagebreak ———————

Encounter data

12. What happens to the data that the CWA collects?
[randomized order, 7-point Likert scale, ranging from "fully agree" to "fully disagree" + " I do not know", single-choice for each item]:

    (a) The RKI uses the data to monitor the infection incidence. ✗
    (b) Third parties use the data to create profiles for commercial purposes (e.g., for personalized advertising) from me. ✗
    (c) The data will be used to monitor my location (and my activities). ✗
    (d) My data will be used to warn me and others in the event of a risk encounter. ✓

———————— Pagebreak ————————

The following part concerns information about the people you have encountered ("encounter data"). This has nothing to do with the information on whether someone is infected.

13. The CWA tracks who I encounter using the following technologies: *[randomized order, 7-point Likert scale, ranging from "fully agree" to "fully disagree" + " I do not know", single-choice for each item]*:
    (a) Mobile data ✗
    (b) WiFi ✗
    (c) Satellite ✗
    (d) Bluetooth ✓
    (e) GPS ✗
14. The CWA requires permanent access to the Internet ✗
    [7-point Likert scale, ranging from "fully agree" to "fully disagree" + " I do not know", single-choice].

———————— Pagebreak ————————

15. The following actors have access to the encounter data collected by the app:
    [randomized order, 7-point Likert scale, ranging from "fully agree" to "fully disagree" + " I do not know", single-choice for each item]:
    (a) The health departments ✗
    (b) Those involved in the development of the CWA ✗
    (c) The Robert Koch Institute ✗
    (d) Hackers ✗
    (e) The federal government ✗
    (f) Others:
16. To what extent do you agree with the following statements about encounter data (i.e., the information about which people you have encountered) in the CWA:
    [randomized order, 7-point Likert scale, ranging from "fully agree" to "fully disagree" + " I do not know", single-choice for each item]:
    (a) The encounter data will only be stored locally on my smartphone. ✓

(b) The encounter data are transferred from user A to user B via a server or cloud. ✗

(c) The encounter data are transferred directly between the smartphones of the users. ✗

(d) The encounter data are uploaded to a server or to a cloud. ✗

———————— Pagebreak ————————

17. How long is encounter data stored (regardless of storage location)? *[single-choice]*?

(a) My encounter data are not stored at all. ✗

(b) My encounter data are stored temporarily. ✓

(c) My encounter data are stored permanently. ✗*

———————— Pagebreak ————————

18. To what extent do you believe the following statements about the CWA are true?
[randomized order, 7-point Likert scale, ranging from "fully agree" to "fully disagree" + " I do not know", single-choice for each item]:

(a) My encounter data will only be transferred to another device (smartphone/server/cloud) if I am infected. ✗

(b) Where my encounter data will be transferred is independent of whether I am infected or not. ✓

(c) The encounter data can always be assigned to me as a person. ✗

———————— Pagebreak ————————

Infection status

19. *[Attention check]*: Research has shown that participants do not always follow the instructions and questions in a survey. To help us monitor the quality of our data, please select "Strongly disagree" from the choices below.
[single-choice, 5-point Likert scale]

- To help us with monitoring the quality of our data, please select "Strongly disagree".

—————— Pagebreak ——————

The following part of the questionnaire is about the information on whether a person is infected ("infection status"). You can assume that a positive test result (i.e., someone is infected) is already stored in the app or has been scanned.

20. The following actors have access to my infection status recorded in the app:
[randomized order, 7-point Likert scale, ranging from "fully agree" to "fully disagree" + " I do not know", single-choice for each item]:
    (a) The health departments ✗
    (b) Those involved in the development of the CWA ✗
    (c) The Robert Koch Institute ✗
    (d) Hackers ✗
    (e) The federal government ✗
    (f) Others:
21. To what extent do you believe the following statements about the CWA are true?
[randomized order, 7-point Likert scale, ranging from "fully agree" to "fully disagree" + " I do not know", single-choice for each item]:
    (a) My infection status is directly linked to my identity in the app. ✗
    (b) The infection status is transferred from user A to user B via a server or cloud. ✓
    (c) Through the app, I can always find out the identity of people tested positively I have encountered. ✗
    (d) If I am infected, the people I encountered before are automatically warned. ✗
    (e) If I am infected, I have to manually agree so that the people I have encountered before are warned. ✓
    (f) The infection status is transferred directly between the smartphones of the users. ✗
    (g) If I share a positive test, I share my identity/name. ✗

—————— Pagebreak ——————

22. To what extent is your infection status stored (regardless of location)? *[single-choice]*?

(a) My infection status is not saved at all. ✗

(b) My infection status is saved temporarily. ✓

(c) My infection status is saved permanently. ✗

———————— Pagebreak ————————

Further knowledge/assessment apart from encounter data and infection status

The following part of the questionnaire is no longer about a specific piece of information or specific data such as infection status or encounter data but about the CWA in general.

23. To what extent do you believe the following statements about the CWA are true?
[randomized order, 7-point Likert scale, ranging from "fully agree" to "fully disagree" + " I do not know", single-choice for each item]:

(a) I think the app is useful in the fight against the pandemic.

(b) The app can warn me directly if an infected person is standing next to me. ✗

(c) My risk status is calculated directly on my smartphone. ✓

(d) I use the app to protect myself.

(e) I am usually warned one or more days later when I have had a risk encounter. ✓

(f) Privacy played an important role for me in deciding whether to install the app.

(g) My risk status is calculated on a server or in a cloud. ✗

(h) I used the app to protect myself.

(i) If everyone can see the program code of the CWA (open source), the app becomes insecure.

(j) The program code of the CWA is publicly available on the internet (open source). ✓

(k) I used the app to protect others.

(l) The app shows me on a map where infected people are located. ✗

(m) I use the app to protect others.

———————— Pagebreak ————————

Based on the information provided by the German government, we would now like to inform you what data the CWA collects for contact tracing: (Figure C.1)

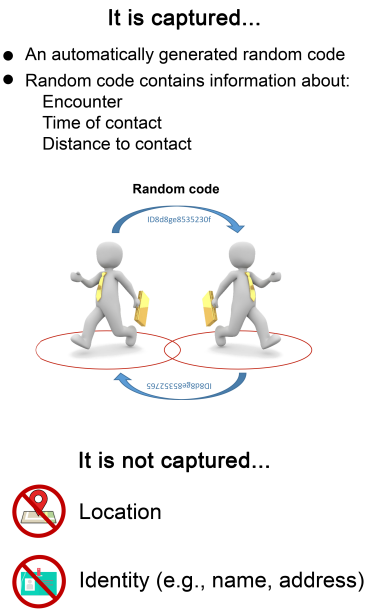


FIGURE C.1: Explanation of the CWA functionality that was shown to the participants during the survey.

———————— Pagebreak ————————

Trust in CWA and public information

24. To what extent do you agree with the following statements about the CWA? *[randomized order, 7-point Likert scale, ranging from "fully agree" to "fully disagree" + " I do not know", single-choice for each item]*:

    (a) Information about the CWA is provided openly and honestly by official bodies (e.g., the German government, RKI).

    (b) The officially published information (e.g., from the German government, RKI) about the CWA is correct.

———————— Pagebreak ————————

25. To what extent do you agree with the following statements about the CWA? *[randomized order, 5-point Likert scale, ranging from "fully agree"to "fully disagree", single-choice for each item, based on Gulati et al.* [95]]

    (a) I feel that I need to be careful when using the CWA.

(b) I believe that the CWA has all the features that I would expect from a contact tracing app.

(c) I think that the CWA fulfills its role as a contact tracing app very well.

(d) I believe that the use of the CWA could have negative consequences.

(e) When I use the CWA, I think I can rely on it completely.

(f) I believe that the CWA is interested in understanding my needs and preferences.

(g) I believe that the CWA will act in my best interest.

(h) I believe that the CWA will do its best to help me when I need help.

(i) I can trust the information that the CWA has given me.

(j) I think the CWA is competent and effective at contact tracing.

(k) I can always rely on the CWA for contact tracing.

(l) It is risky to interact with the CWA.

———————— Pagebreak ————————

Usage of features

26. Which features of the CWA do you use?
[randomized order, multiple choice]

(a) Quick test profile

(b) Scanning of a test result (both positive and negative)

(c) Tracking of local incidences

(d) Sharing a positive test result

(e) Contact Journal

(f) Encounter notifications/risk calculation

(g) Check-in

(h) Deposit of vaccination certificates

(i) None

———————— Pagebreak ————————

27. Which features of the CWA have you used in the past but do not currently use?
[randomized order, multiple choice]

(a) Quick test profile
(b) Scanning of a test result (both positive and negative)
(c) Tracking of local incidences
(d) Sharing a positive test result
(e) Contact Journal
(f) Encounter notifications/risk calculation
(g) Check-in
(h) Deposit of vaccination certificates
(i) None

———————— Pagebreak ————————

Dark triad personality traits

Thank you for your responses so far.
The following questions no longer refer to the CWA but to your personal attitudes and feelings.

28. Short Dark Triad measure [117, 140]
[randomized order, 7-point Likert scale, ranging from "fully agree" to "fully disagree", single-choice for each item]

- Machiavellianism
  (a) It's not wise to tell your secrets.
  (b) I like to use clever manipulation to get my way.
  (c) Whatever it takes, you must get the important people on your side.
  (d) Avoid direct conflict with others because they may be useful in the future.
  (e) It's wise to keep track of information that you can use against people later.
  (f) You should wait for the right time to get back at people.
  (g) There are things you should hide from other people to preserve your reputation.
  (h) Make sure your plans benefit yourself, not others.
  (i) Most people can be manipulated.
- Narcissism
  (a) People see me as a natural leader.

(b) I hate being the center of attention. (R)
(c) Many group activities tend to be dull without me.
(d) I know that I am special because everyone keeps telling me so.
(e) I like to get acquainted with important people.
(f) I feel embarrassed if someone compliments me. (R)
(g) I have been compared to famous people.
(h) I am an average person. (R)
(i) I insist on getting the respect I deserve.

- Psychopathy
  (a) I like to get revenge on authorities.
  (b) I avoid dangerous situations. (R)
  (c) Payback needs to be quick and nasty.
  (d) People often say I'm out of control.
  (e) It's true that I can be mean to others.
  (f) People who mess with me always regret it.
  (g) I have never gotten into trouble with the law. (R)
  (h) I enjoy having sex with people I hardly know.
  (i) I'll say anything to get what I want.

———————— Pagebreak ————————

29. *[Attention check]*: It is important that you pay attention to the statements. Please agree by selecting "Strongly agree".
[single-choice, 7-point Likert scale, ranging from "fully agree" to "fully disagree" + " I do not know"]

    - I pay attention to the questions in this questionnaire. I confirm this by selecting "Strongly agree".

———————— Pagebreak ————————

Privacy concerns

30. IUIPC-8 [93]
[randomized order, 7-point Likert scale, ranging from "fully agree" to "fully disagree", single-choice for each item]:

    (a) When online companies ask me for personal information, I sometimes think twice before providing it.

(b) It bothers me to give personal information to so many online companies.

(c) Consumer control of personal information lies at the heart of consumer privacy.

(d) A good consumer online privacy policy should have a clear and conspicuous disclosure.

(e) I'm concerned that online companies are collecting too much personal information about me.

(f) It usually bothers me when online companies ask me for personal information.

(g) Companies seeking information online should disclose the way the data are collected, processed, and used.

(h) Consumer online privacy is really a matter of consumers' right to exercise control and autonomy over decisions about how their information is collected, used, and shared.

———————— Pagebreak ————————

31. Thank you very much for your reply! If you would like to leave us another comment, you can do so below:
[open-ended]

C.2 Additional Tables and Figures

Survey Results from the Kruskal-Wallis tests

	df	H-value	Sig.
Access to location data			
Companies involved in the CWA development	2	7.111	.029*
Government	2	9.387	.009**
RKI	2	9.585	.008**
Public health departments	2	9.14	.01*
Hacker	2	11.603	.003**
Access to demographic information			
Companies involved in the CWA development	2	0.261	.878
Government	2	0.318	.853
RKI	2	2.457	.293
Public health departments	2	0.768	.681
Hacker	2	3.926	.14
Access to encounter data			
Companies involved in the CWA development	2	9.481	.009**
Government	2	5.442	.066
RKI	2	6.319	.042*
Public health departments	2	4.781	.092
Hacker	2	27.819	<.001**
Access to infection status			
Companies involved in the CWA development	2	17.984	<.001**
Government	2	5.747	.056
RKI	2	8.399	.015*
Public health departments	2	9.178	.01*
Hacker	2	24.214	<.001**

*Note: *p<.05, **p<.01, ***p<.001*

TABLE C.1: Results of Kruskal-Wallis tests comparing users', past users', and non-users' answers to items covering who has access to what data. Statistically significant concepts were further tested for group differences by Mann-Whitney-U-tests. "df" stands for degrees of freedom.

	df	H-value	Sig.
S1: Correct technology for encounter detection [Bluetooth]	2	18.245	<.001**
S2: Incorrect technology for encounter detection	2	19.531	<.001**
Q9a: Location	2	11.247	.004**
Q9b: IP address	2	8.737	.013*
Q9c: Information about app usage	2	15.811	<.001**
Q9d: Distance to others	2	7.459	.024*
Q9e: Demographic information	2	24.792	<.001**
Q9f: Phone model	2	1.827	.401
Q9g: Random codes	2	6.940	.031*
Q9h: Duration of contact	2	6.757	.034*
Q9i: Infection status	2	1.291	.525
Q9j: Time of contact	2	0.170	.919*
S3: Identity can be assigned to infection status	2	26.536	<.001**
S4: Identity can be assigned to encounter data	2	13.362	.001**
S5: Data are only used to warn others	2	2.333	.311
S6: Data are used to monitor infection incidence	2	2.896	.235
S7: Data are used to create advertising profiles	2	11.537	.003**
S8: Data are used to monitor the user's location	2	25.857	<.001**
S9: Data transmission and storage via server	2	4.056	.132
S10: Data transfer directly between smartphones	2	0.349	.840
S11: Local data storage	2	9.65	.008**
S12: Local calculation of risk status	2	8.375	.015*
S13: Data transmission is independent of infection status	2	9.542	.008**
S14: Only data from infected people is transferred to server	2	6.53	.038*
S15: Infected are displayed on a map	2	22.871	<.001**
S16: Warning usually with delay	2	10.206	.006**
S17: Automatic warning after positive test	2	5.876	.053
S18: Warning only after manual approval	2	12.73	.002**
	df	H-value	Sig.
Gulati et al.	2		
S19: Risk	2	55.942	<.001**
S20: Benevolence	2	38.718	<.001**
S21: Competence	2	55.037	<.001**
S22: Trust	2	67.976	<.001**
Misc.	2		
S23: Official information about CWA is true	2	32.681	<.001**
S24: CWA is useful in pandemic response	2	78.174	<.001**
S25: Data protection was important for decision for/against CWA use	2	0.568	.753
S26: CWA code is open source	2	2.272	.321
S27: Open source is insecure	2	11.127	.004**

*Note: *p<.05, **p<.01, ***p<.001*

TABLE C.2: Results of Kruskal-Wallis tests comparing users', past users', and non-users' answers to scales covering various dimensions of what the CWA can da and how the app is perceived. Statistically significant concepts were further tested for group differences by Mann-Whitney-U-tests. "df" stands for degrees of freedom.

Survey Scale Development

	Cronbach's alpha
S1: Correct technology for encounter detection [Bluetooth]	
S2: Incorrect technology for encounter detection	.846
- The CWA tracks who I encounter using the following technologies...	
- Mobile data (Q13a)	
- WiFi (Q13b)	
- Satellite (Q13c)	
- GPS (Q13e)	
- The CWA requires permanent access to the Internet. (Q14)	
S3: Identity can be assigned to infection status	.841
- My infection status is directly linked to my identity in the app. (Q21a)	
- Through the app, I can always find out the identity of people tested positively I have encountered. (Q21c)	
- If I share a positive test, I share my identity/name. (Q21g)	
S4: Identity can be assigned to encounter data	
- The encounter data can always be assigned to me as a person. (Q18c)	
S5: Data are used to warn me and others	
- My data will be used to warn me and others in the event of a risk encounter. (Q12d)	
S6: Data are used to monitor infection incidence	
- The RKI uses the data to monitor the infection incidence. (Q12a)	
S7: Data are used to create advertising profiles	
- Third parties use the data to create profiles for commercial purposes (e.g., for personalized advertising) from me. (Q12b)	
S8: Data are used to monitor the user's location	
- The data will be used to monitor my location (and my activities). (Q12c)	
- The CWA tracks who I encounter using the following technologies... Bluetooth (Q13d)	
S9: Data transmission and storage via server	.836
- The encounter data are transferred from user A to user B via a server or cloud. (Q15b)	
- The encounter data are uploaded to a server or to a cloud. (Q15d)	
- The infection status is transferred from user A to user B via a server or cloud. (Q21b)	
- My risk status is calculated on a server or in a cloud. (Q23g)	

Continued on next page

Table C.3 – *Continued from previous page*

	Cronbach's alpha
S10: Data transfer directly between smartphones	.700
- The encounter data are transferred directly between the smartphones of the users. (Q16c)	
- The infection status is transferred directly between the smartphones of the users. (Q21f)	
S11: Local storage of encounter data	
- The encounter data will only be stored locally on my smartphone. (Q16a)	
S12: Local calculation of risk status	
- My risk status is calculated directly on my smartphone. (Q21c)	
S13: Data transmission is independent of infection status	
- Where my encounter data will be transferred to is independent of whether I am infected or not. (Q18b)	
S14: Only data from infected people is transferred to server	
- My encounter data will only be transferred to another device (smartphone/server/cloud) if I am infected. (Q18a)	
S15: Detector of infected persons	.759
- The app shows me on a map where infected people are located. (Q23l)	
- The app can warn me directly if an infected person is standing next to me. (Q23b)	
S16: Warning usually with delay	
- I am usually warned one or more days later when I have had a risky encounter. (Q23e)	
S17: Automatic warning after positive test	
- If I am infected, the people I encountered before are automatically warned. (Q21d)	
S18: Warning only after manual approval	
- If I am infected, I have to manually agree so that the people I have encountered before are warned. (Q21e)	
S19: Risk	.897
- I feel that I need to be careful when using the CWA. (Q25a)	
- I believe that the use of the CWA could have negative consequences. (Q25d)	
- It is risky to interact with the CWA. (Q25o)	
S20: Benevolence	.666
- I believe that the CWA will act in my best interest. (Q25k)	
- I believe that the CWA will do its best to help me when I need help. (Q25k)	
- I believe that the CWA is interested in understanding my needs and preferences. (Q25i)	

Continued on next page

Table C.3 – *Continued from previous page*

	Cronbach's alpha
S21: Competence	.868
- I think the CWA is competent and effective at contact tracing. (Q25m)	
- I think that the CWA fulfills its role as a contact tracer very well. (Q25c)	
- I believe that the CWA has all the features that I would expect from a contact tracing app. (Q25b)	
S22: Trust	.871
- When I use the CWA, I think I can rely on it completely. (Q25h)	
- I can always rely on the CWA for contact tracing. (Q25n)	
- I can trust the information that the CWA has given me. (Q25l)	
S23: Official information about CWA is true	.917
- Information about the CWA is provided openly and honestly by official bodies (e.g., the German government, RKI). (Q24a)	
- The officially published information (e.g., from the German government, RKI) about the CWA is correct. (Q24b)	
S24: CWA is useful in pandemic response	
- I think the app is useful in the fight against the pandemic. (Q23a)	
S25: Data protection was important for decision for/against CWA use	
- Data protection played an important role for me in deciding whether to install the app. (Q23f)	
S26: CWA code is open source	
- The program code of the Corona-Warn-App is publicly available on the internet (open source). (Q23j)	
S27: Open source is insecure	
- If everyone can see the program code of the CWA (open source), the app becomes insecure. (Q23i)	

TABLE C.3: This table lists the composition of scales we built to provide a summary measure and reports Cronbach's alphas. The scale components are determined by factor analysis followed by manual separation into thematic matches as described in Section 2.4.2.

C.3 Interview Study

The content of this section is not based on my research but provided because the study presented in Section 2.4 is easier understood with the results of the interviews at hand. I was not involved in the design nor the analysis of the interviews.

C.3.1 Interviews Study

We wanted to gain an understanding of CWA users' and non-users' mental models in terms of data collection and processing in the app and relevant entities to evaluate how *informed* participants are about these processes. To this end, we conducted 20 semi-structured interviews, where 10 participants were users and 10 were non-users of the CWA[1]. The interviews took place between the 5th and 26th of July 2021. All interviews were conducted and recorded using Zoom. We conducted two pilot interviews with participants recruited from our personal contacts to confirm the clarity and comprehensibility of study materials and refine the interview questions and instructions based on the feedback and our own impressions during the pilot interviews. In the following section, we describe the methodology and interview results.

Method

Participants and Recruitment The participants were recruited via posters placed around our university campus as well as in restaurants and grocery stores in a city in Germany. Additionally, we employed online platforms such as SurveyCircle[2] and word of mouth for recruitment. Our aim was to ensure a balanced sample in terms of CWA (non-)usage, self-identified gender, and age. To be eligible for study inclusion, participants had to own a smartphone and reside in Germany. We proceeded to recruit participants until no significant new ideas emerged during the interviews, resulting in a final sample of 20 participants (10 CWA users and 10 CWA non-users). Although we conducted the interviews before a complete coding process, the approach was validated as no new themes and codes emerged after we had coded 16 participants.

[1] We reached data saturation after 16 interviews; eight interviews each with CWA users and non-users.

[2] `https://www.surveycircle.com`, visited August 11, 2022

	Users vs. Non-Users		Users vs. Past Users		Past Users vs. Non-Users		Privacy Concerns (≤25% vs. ≥75%) Awareness		Collection		Control	
	Z	r	Z	r	Z	r						
S1: Correct technology for encounter detection [Bluetooth]	-3,73**	.23	-0.54		-3.24**	.25	-2.26*	.16	-1.20		-2.22*	.16
S2: Incorrect technology for encounter detection	-4.43**	.26	-0.64		-2.13†		-0.26		-0.63		-1.18	
Q9a: Location	-2.76**	.16	-0.81		-2.85**	.21	-4.72**	.32	-2.94**	.21	-1.07	
Q9b: IP address	-3.00**	.19	-0.78		-1.22		-0.59		-0.13		-1.09	
Q9c: Information about app usage	-3.48**	.22	-0.55		-3.07**	.23	-1.48		-2.06*	.16	-0.29	
Q9d: Distance to others	-2.72**	.16	-1.12		-0.82		-2.18*	.15	-0.40		-2.24*	.16
Q9e: Demographic information	-4.90**	.30	-0.87		-2.58*	.19	-1.76		-0.24		-1.66	
Q9f: Phone model	-1.25		-0.02		-0.92		-2.68**	.19	-1.11		-1.72	
Q9g: Random code	-2.48*	.17	-1.69		-0.06		-0.18		-0.05		-0.05	
Q9h: Duration of contact	-2.61**	.16	-0.72		-1.05		-3.79**	.26	-1.27		-2.01*	.15
Q9i: Infection status	-1.04		-0.11		-0.81		-5.16**	.35	-1.98*	.14	-2.88**	.20
Q9j: Time of contact	-0.02		-0.38		-0.39		-4.62**	.31	-2.86**	.20	-3.25**	.23
S3: Identity can be assigned to infection status	-5.06**	.30	-2.36*	.17	-1.68		-3.78**	.25	-1.16		-2.94**	.21
S4: Identity can be assigned to encounter data	-3.61**	.22	-0.99		-1.75		-0.09		-1.14		-1.01	
S5: Data is only used to warn others	-0.97		-0.74		-1.43		-8.34**	.55	-4.20**	.30	-5.95**	.41
S6: Data is used to monitor infection incidence	-0.44		-1.69		-1.40		-4.16**	.28	-2.66**	.19	-2.21*	.16
S7: Data is used to create advertising profiles	-3.41**	.20	-1.07		-1.26		-4.65**	.32	-1.26		-3.20**	.23
S8: Data is used to monitor the user's location	-4.93**	.29	-1.17		-2.76**	.20	-2.78**	.19	-0.19		-2.53*	.18
S9: Data transmission and storage via server	-1.84		-0.19		-1.43		-1.44		-1.97*	.15	-0.59	
S10: Data transfer directly between smartphones	-0.59		-0.18		-0.24		-1.92		-0.64		-2.41*	.17
S11: Local storage of encounter data	-2.55*	.16	-2.56*	.20	-0.83		-0.76		-0.08		-0.71	
S12: Local calculation of risk status	-2.56*	.17	-0.35		-2.19†		-0.65		-0.65		-0.36	
S13: Data transmission is independent of infection status	-2.97**	.19	-1.89		-0.24		-0.17		-0.71		-0.32	
S14: Only data from infected people is transferred to server	-2.38†		-1.74		-0.15		-1.24		-0.82		-0.22	
Access to location data (Q10)												
a: Companies involved in the CWA development	-2.46*	.16	-1.87		-0.26		-1.12		-2.58*	.21	-0.53	
b: Government	-3.03**	.21	-0.44		-1.45		-2.06*	.16	-0.31		-2.48*	.21
c: RKI	-3.05**	.21	-1.61		-0.38		-0.19		-1.36		-0.77	
d: Public health departments	-2.96**	.20	-1.68		-0.03		-0.19		-1.08		-0.59	
e: Hacker	-3.38**	.24	-1.34		-1.08		-0.80		-1.00		-0.95	
Access to demographic information (Q11)												
a: Companies involved in the CWA development	-0.09		-0.34		-0.54		-1.44		-1.37		-1.68	
b: Government	-0.02		-0.53		-0.52		-0.21		-0.49		-0.05	
c: RKI	-0.35		-1.22		-1.54		-2.68**	.27	-1.59		-1.56	
d: Public health departments	-0.87		-0.51		-0.15		-2.89**	.29	-0.66		-2.60**	.28
e: Hacker	-1.92		-0.5		-0.95		-1.02		-2.36*	.27	-0.85	
Access to encounter data (Q15)												
a: Companies involved in the CWA development	-2.74**	.17	-0.18		-2.25*	.17	-0.23		-1.68		-0.86	
b: Government	-2.23†		-1.47		-0.01		-2.24*	.16	-0.16		-2.67**	.19
c: RKI	-1.98†		-2.08†		-0.92		-2.06*	.14	-1.78		-0.15	
d: Public health departments	-2.14†		-1.25		-0.17		-1.88		-1.46		-0.47	
e: Hacker	-5.27**	.33	-1.65		-2.04†		-1.81		-0.74		-1.23	
Access to infection status (Q20)												
a: Companies involved in the CWA development	-4.01**	.24	-0.44		-2.65**	.20	-0.12		-1.58		-1.59	
b: Government	-2.34†		-1.03		-0.93		-2.49*	.17	-0.74		-3.01**	.22
c: RKI	-2.94**	.18	-1.12		-0.77		-2.01*	.14	-1.12		0	
d: Public health departments	-3.00**	.18	-0.48		-1.59		-1.35		-0.82		-0.43	
e: Hacker	-4.86**	.30	-1.28		-2.30*	.18	-0.77		-1.12		-0.80	
S15: Detector of infected persons	-4.39**	.26	-0.13		-3.29**	.24	-2.71**	.18	-0.70		-3.12**	.22
S16: Warning usually with delay	-3.18**	.20	-1.11		-1.15		-2.25*	.16	-1.75		-2.60**	.20
S17: Automatic warning after positive test	-2.13†		-1.79		-0.32		-5.19**	.35	-3.13**	.22	-3.75**	.27
S18: Warning only after manual approval	-2.14†		.33**	.26	-2.03†		-1.50		-0.28		-1.14	
S19: Risk	-7.43**	.43	-3.09**	.22	-2.41*	.17	-1.23		-2.45*	.17	-1.41	
S20: Benevolence	-5.75**	.33	-4.26**	.30	-0.16		-1.97*	.13	-1.41		-0.38	
S21: Competence	-7.38**	.43	-3.75**	.26	-0.89		-0.06		-1.00		-0.94	
S22: Trust	-7.84**	.45	-5.13**	.36	-0.59		-0.98		-1.54		-1.01	
S23: Official information about CWA is true	-5.62**	.33	-3.00**	.21	-1.02		-3.47**	.24	-1.75		-4.25**	.30
S24: CWA is useful in pandemic response	-8.39**	.49	-5.50**	.39	-1.30		-0.03		-0.34		-0.49	
S25: Data protection was important for decision for/against CWA use	-0.07		-0.73		-0.67		-3.64**	.24	-5.84**	.42	-2.30*	.16
S26: CWA code is open source	-1.21		-1.24		-0.47		-0.12		-0.51		-0.94	
S27: Open source is insecure	-3.27**	.21	-0.89		-1.70		-0.81		-1.35		-0.62	

*Note: *p<.05, **p<.01, ***p<.001, †=p>.05 after correction for multiple testing;* r=effect size

TABLE C.4: This table shows the detailed results of Mann-Whitney-U-tests already shown in Table 2.10 comparing the scales resulting from our analysis covering various mental model concepts (anonymity, data use, technology, data transmission, data storage, warnings) of users, past users, non-users, and participants with low (≤25%) and high (≥75%) privacy concerns (PC). For each concept and group, we report Z and the corresponding r.

	1	2	3	4	5	6	7	8	9	10	11
If I share a positive test, I share my identity/name.	.806	-.068	-.029	.125	.062	-.083	.006	-.051	-.069	.000	-.086
My infection status is directly linked to my identity in the app.	.805	-.151	-.058	.122	.055	.007	.020	.013	.076	.138	-.121
Through the app, I can always find out the identity of people tested positively I have encountered.	.801	-.014	.022	.182	-.117	.015	.198	-.106	.023	.082	.012
The data will be used to monitor my location (and my activities).	.777	-.004	.025	.198	-.159	.048	.152	.271	-.030	.011	-.002
The app shows me on a map where infected people are located.	.733	.132	.130	.266	-.087	.079	.064	.063	.130	-.039	.124
Third parties use the data to create profiles for commercial purposes (e.g., for personalized advertising) from me.	.705	-.024	.046	.180	-.232	.120	.275	.269	-.061	.043	-.086
It is risky to interact with the CWA.	.700	-.178	-.110	.067	-.037	.006	.123	-.047	.023	-.364	-.070
The encounter data can always be assigned to me as a person.	.651	-.064	.053	.275	.035	-.061	-.226	.330	.154	.015	.110
I believe that the use of the CWA could have negative consequences.	.627	-.242	-.179	.173	.015	-.044	.063	.004	-.020	-.390	.023
I feel that I need to be careful when using the CWA.	.607	-.229	-.038	.028	.087	.004	-.012	.016	-.070	-.398	.112
The app can warn me directly if an infected person is standing next to me.	.545	.196	.088	.192	-.008	.074	-.214	.060	.019	-.017	.366
Where my encounter data will be transferred is independent of whether I am infected or not.	.518	-.084	-.024	.217	.131	.189	-.094	.209	.148	.038	.038
If everyone can see the program code of the CWA (open source), the app becomes insecure.	.476	.161	.145	.232	.105	.087	-.246	.129	.051	.059	.181
The encounter data is transferred from user A to user B via a server or cloud.	.471	-.062	.117	.148	.216	-.258	.221	.401	.262	-.085	.032
I think the CWA is competent and effective at contact tracing.	-.110	.853	.247	.048	.071	.065	-.112	-.018	.118	.012	-.400
I can always rely on the CWA for contact tracing.	.022	.826	.087	-.002	-.022	-.016	.039	-.036	-.073	.021	.022
I think that the CWA fulfills its role as a contact tracer very well.	-.086	.809	.101	-.055	.154	.033	-.008	.019	-.064	-.041	-.046
I believe that the CWA will act in my best interest.	-.306	.772	.113	.008	.048	.135	.122	.085	-.046	-.038	.171
I believe that the CWA has all the features that I would expect from a contact tracing app.	-.045	.708	.038	-.143	.156	.204	-.139	.052	.033	.037	-.013
I believe that the CWA will do its best to help me when I need help.	.011	.706	.281	.034	.031	.029	-.012	.048	.136	.096	.078
When I use the CWA, I think I can rely on it completely.	.065	.694	.209	-.002	-.148	.005	.058	.060	-.092	-.019	.149
I can trust the information that the CWA has given me.	-.145	.694	.161	.067	.085	.008	.083	-.038	-.022	.107	.103
I think the app is useful in the fight against the pandemic.	-.066	.618	.448	.026	.039	.015	-.041	.085	-.003	.012	-.117
Information about the CWA is provided openly and honestly by official bodies (e.g., the German government, RKI).	-.346	.551	.127	.001	.316	.239	.206	-.032	-.118	.407	.061
The officially published information (e.g., from the German government, RKI) about the CWA is correct.	-.277	.550	.160	.034	.420	.211	.230	-.110	-.122	.319	.053
I believe that the CWA is interested in understanding my needs and preferences.	.278	.467	.029	.058	-.094	-.165	.079	-.097	.099	.007	-.040
The encounter data will only be stored locally on my smartphone.	-.188	.378	.060	.022	-.190	.234	.264	-.230	.231	.130	.044
My risk status is calculated directly on my smartphone.	.111	.302	.054	.204	-.042	.218	.189	-.177	-.026	.246	-.019
I used the app to protect others.	-.040	.266	.840	-.045	-.023	.145	.075	.104	.111	.130	.028
I use the app to protect others.	.004	.397	.805	-.054	-.010	.025	.152	.106	.015	.087	-.034
I used the app to protect myself.	.034	.289	.750	-.057	.048	-.075	.150	-.030	-.018	-.006	.103
I use the app to protect myself.	.084	.453	.725	-.001	.007	-.004	.222	-.006	-.157	-.111	-.078
Privacy played an important role for me in deciding whether to install the app.	.058	.279	.332	.253	.236	.051	.002	-.023	.226	-.049	.290
The CWA tracks who I encounter using the following technologies: - Mobile data.	.247	-.045	-.004	.813	.105	-.006	-.004	.048	.010	.112	.018
The CWA tracks who I encounter using the following technologies: - GPS.	.187	.041	-.129	.807	.152	.009	.020	.051	.020	-.122	-.055
The CWA tracks who I encounter using the following technologies: - Wi-Fi	.343	-.060	.066	.643	.019	.106	.089	.076	.046	.023	-.021
The CWA tracks who I encounter using the following technologies: - Satellite	.393	.089	.017	.604	-.049	.063	.007	.261	.021	.006	.063
The CWA requires permanent access to the Internet	.363	-.020	-.109	.562	.011	-.087	-.061	-.135	-.073	-.045	.105
My data will be used to warn me and others in the event of a risk encounter.	-.316	.099	.053	.043	.709	.109	.081	-.103	.046	-.069	.018
If I am infected, the people I encountered before are automatically warned.	.075	.013	-.005	.075	.606	-.018	-.038	.073	.079	.048	.020
The RKI uses the data to monitor the infection incidence.	.142	.186	.018	.122	.437	.030	-.027	.200	.017	-.016	-.016
If I am infected, I have to manually agree so that the people I have encountered before are warned.	.090	.267	.065	.190	-.294	.168	.191	-.099	.089	.026	.119
The encounter data are transferred directly between the smartphones of the users.	.052	.126	-.056	.059	.045	.682	.071	.019	.001	.042	.106
The infection status is transferred directly between the smartphones of the users.	.168	.104	.052	.121	-.014	.668	-.171	-.186	-.224	.052	-.102
The CWA tracks who I encounter using the following technologies: - Bluetooth	-.071	-.014	.311	-.238	.096	.480	.206	-.028	.153	-.098	-.074
I am usually warned one or more days later when I have had a risk encounter.	.130	-.060	.209	.000	.124	-.207	.619	.038	.015	.105	-.109
The program code of the Corona-Warn app is publicly available on the internet (open source).	.098	.045	.098	.008	-.036	.112	.446	.009	.016	-.111	.055
My encounter data will only be transferred to another device (smartphone/server/cloud) if I am infected.	-.022	.265	.130	.033	-.072	.066	.388	.007	.131	.153	-.005
The encounter data are uploaded to a server or to a cloud.	.539	-.035	.088	.116	.232	-.069	-.038	.615	.053	-.117	-.007
My risk status is calculated on a server or in a cloud.	.368	.178	.192	.176	.106	-.208	.069	.543	.144	.089	.011
The infection status is transferred from user A to user B via a server or cloud.	.376	-.102	.018	.021	.301	-.207	.222	.261	.715	-.012	.006

TABLE C.5: This table shows the matrix of factor loadings from the factor analysis (extraction method: maximum likelihood, rotation method: Varimax with Kaiser normalization).

ID	Age	Gender	Occupation	Highest education	OS	Mental model
user1	51–60	m	Technical clerk	PhD or higher	Android	advanced
user2	21–30	m	Engineer	Bachelor/Master Degree	Android	central server
user3	51–60	f	Doctor	PhD or higher	iOS	simple
user4	51–60	m	Business consultant (Manager)	PhD or higher	Android	simple
user5	61–70	m	Privateer	PhD or higher	Android	advanced
user6	51–60	m	NA	Bachelor/Master Degree	iOS	advanced
user7	21–30	f	Teacher	Bachelor/Master Degree	Android	local
user8	51–60	f	Psychological counselor	High School Diploma	Android	simple
user9	31–40	f	Retail salesperson	PhD or higher	Android	central server
user10	21–30	m	Gastronomer	Bachelor/Master Degree	iOS	central server
nonuser1	61–70	m	Software developer (Manager)	PhD or higher	Android	local
nonuser2	21–30	m	Retail salesperson	High School Diploma	Android	central server
nonuser3	21–30	f	Child therapist (in training)	Bachelor/Master Degree	iOS	simple
nonuser4	61–70	f	Seamstress	High School Diploma	Android	central server
nonuser5	21–30	f	Nurse and nursing educator	Bachelor/Master Degree	Android	local
nonuser6	51–60	f	Key account manager	Bachelor/Master Degree	Android	central server
nonuser7	21–30	m	CNC specialist	High School Diploma	Android	central server
nonuser8	31–40	f	Event manager	High School Diploma	iOS	central server
nonuser9	>70	f	Pensioner	Bachelor/Master Degree	iOS	central server
nonuser10	51–60	f	Teacher	Bachelor/Master Degree	Android	simple

TABLE C.6: This table presents the interview participants' demographics and lists their mental model of the way the CWA works.

Eleven participants self-identified as women, nine as men, and 14 participants used Android, while the other six used iOS. For detailed demographics, please refer to Table C.6.

All participants were offered a compensation of €10. However, 13 participants waived payment since they volunteered to support the research in this field.

Study Procedure All participants were contacted via email to confirm the inclusion criteria, make interview appointments, and provide the consent form. We asked all participants to send us the signed consent form prior to the interviews.

The interviews consisted of the following six main parts (for the detailed interview script, please refer to Section C.3.1 in the Appendix) and lasted on average 70 minutes (min = 47, max = 109 minutes):

1) We thanked the participants, made sure they had signed the informed consent form, provided them with details about the study procedure, and gave them the opportunity to ask questions.

2) We asked about their experiences with the CWA, including from which sources they had learned about the app, reasons for (not) using the app, privacy concerns associated with using the app, who they thought the app's providers were, and to what extent they trust those providers.

3) We focused on the participants' understanding of the technical functioning of the CWA, i.e., their *informedness* regarding the app's data collection and processing. For this, the participants were given a drawing task where they were asked to describe the transfer, storage, and processing of data within the CWA between two smartphones of users walking past each other in a fictional scenario. Participants had the choice between sketching by hand (16 chose this option) or using the Zoom internal whiteboard function (three chose this option). One of the three participants who initially used the Zoom whiteboard function had to switch to a prepared whiteboard in Miro[3] due to technical problems. One participant found the drawing task useless and thus refused to participate in this task but gave a detailed verbal explanation of how they envisaged the transfer, storage, and processing of data in the described situations. During the drawing task, the participants were asked to express their thoughts freely (i.e., think-aloud). Subsequently, data transmission, storage, and processing, as well as different situations in dealing with the CWA, were discussed in more detail.

4) We used a PowerPoint presentation to explain how the CWA works. This presentation was based on the information provided by the Robert Koch-Institute (RKI) and German government. Participants then had the opportunity to ask questions to make sure they understood the provided information.

5) We inquired again about their trust in the app providers to capture changes in their attitude from the information provided in the initial interview. We also

[3] `https://miro.com`, visited August 11, 2022

asked about their use of other apps, such as messenger and navigation apps, which are at least comparable to the CWA in terms of data collection. Additionally, they were asked if they were risk patients and if they had experienced COVID-19 infections in their personal environment. Non-users were further asked whether their intention to use the CWA had changed during the interview and what conditions would have to be met for them to consider using it.

6) Participants were asked to complete a short questionnaire on their demographic information and were then debriefed and thanked again for their participation in the study.

Data Analysis The interviews and drawings were analyzed using thematic analysis [23]. The researcher who conducted the interviews first read through all the transcribed interviews and looked at the drawings multiple times. They then coded all the interview data at the sentence level, going back and forth multiple times, to develop a codebook. This codebook was discussed with another researcher and refined by two other researchers. Two researchers then used the codebook to code all interview data independently. Finally, they came together to discuss ambiguities and disagreements. During the coding process, we identified four main themes: (1) false assumptions about how the app works, (2) accurate assumptions about how the app works, (3) privacy concerns, and (4) factors influencing app usage. Further, we grouped the explanations of the interviewees as well as the corresponding drawings according to similarities in terms of functioning. In this process, we identified four mental models: (1) advanced technical model, (2) simplified model, (3) server model, and (4) local model. All codes discussed in this paper are given in Table C.8 in the Appendix.

Ethics We received clearance from the institution's Research Ethics Board for the interview study and adhered to the German data protection laws and the GDPR in the EU. All participants provided informed consent for participation and their data being used for research purposes prior to the study. They were told that they could terminate the study at any time without any negative consequences and that, in this case, all data collected from them until that point would be deleted. We also assured them that the collected data would only be used for research purposes, be handled confidentially, and never be linked to their identity. We used Zoom for conducting the interviews, which included the transfer of participant data to servers hosted in the U.S. Still, as Zoom was used via a university license, the university's data processing agreement with Zoom ensured that all data processing adhered to GDPR requirements. Participants were informed beforehand that the interviews would be conducted via Zoom and that they could turn off their cameras during the interviews.

Limitations Like most user studies, our interview study is subject to several limitations.

First, qualitative interview data relies on self-report. Hence, some participants might have over- or understated their privacy concerns or other objections due to social desirability bias.

Second, it is difficult to capture existing mental models without changing them as a result. By asking specific questions about how the app works, we may have triggered thought processes that led participants to form more specific ideas about these functions.

Third, with the pandemic situation changing dynamically, the time at which the interviews were conducted (summer 2021 when the vaccination campaign was in full swing and incidences were rather low in Germany) may also have had an impact on the views of the interviewees, at least in terms of how useful they consider the app to be. We deliberately chose a time when there had already been a lot of media coverage about how the app works, as we were interested in people's understanding of the app after they potentially received prior information. Nevertheless, we are not able to track exactly how much and what information the participants actually actively perceived.

Fourth, although we aimed to balance the sample in terms of demographics (e.g., self-identified gender, age), the sample is biased toward rather well-educated people, particularly in the subsample of CWA users. We further interviewed more Android users than iOS users (still, this distribution reflects the market share of mobile OS in Germany with 66% using Android [224]). All participants were recruited in selected venues from a single city in Germany. The study results should thus be validated using a larger, more representative sample. We take the first step toward this in the survey study (see Section 2.4).

Results

In this section, we present the four mental models of CWA data collection and processing reflecting the participants' informedness about these processes found in our data: the *advanced technical model*, *simplified model*, *server model*, and *local model*. All models are presented graphically and descriptive. Table C.7 additionally presents an overview of the models based on certain elements (e.g., what data is captured).

Even though many models include a few correct assumptions, none of the participants had a completely accurate understanding of the app. After presenting the models, we derive ideas on how the mental models might differ between CWA users and non-users (RQ2) and people with varying levels of privacy concerns (RQ3).

First Model: Advanced Technical Model Three participants (all three CWA users) had an advanced technical mental model (see Figure C.2). They depicted a deep understanding of the exact functioning of the CWA, perhaps due to their professional background in IT, and used the correct technical terms (e.g., "random codes", "encryption", "server"). The exact processes of data transmission

as well as the components involved were consistent with the official explanation provided by the RKI. The three interviewees had only ambiguities regarding data processing. In their opinion, the matching of their own random codes with the random codes of the infected persons took place regularly on the server, but in fact, only the random codes of the infected persons are temporarily stored on the server. What they are referring to is what is called the centralized model. The three users who held the advanced technical mental model neither expressed any privacy concerns nor expected any negative consequences as a result of voluntarily disclosing their infection status based on their expected high level of data protection. However, voluntary disclosure of one's infection status was interpreted not only as an advantage in terms of data protection but also as a limitation of the functioning of the CWA since it made it dependent on the behavior of the users. Two participants even criticized that the increased privacy hindered the functioning, e.g., user8:*"So by doing that [implementing voluntary disclose of one's infection status] probably 30% didn't get a warning at all. At least 30% because people didn't enter it at all. And once because maybe they didn't even think about it. And then maybe also out of fear: If I enter it, then the others might notice it."*

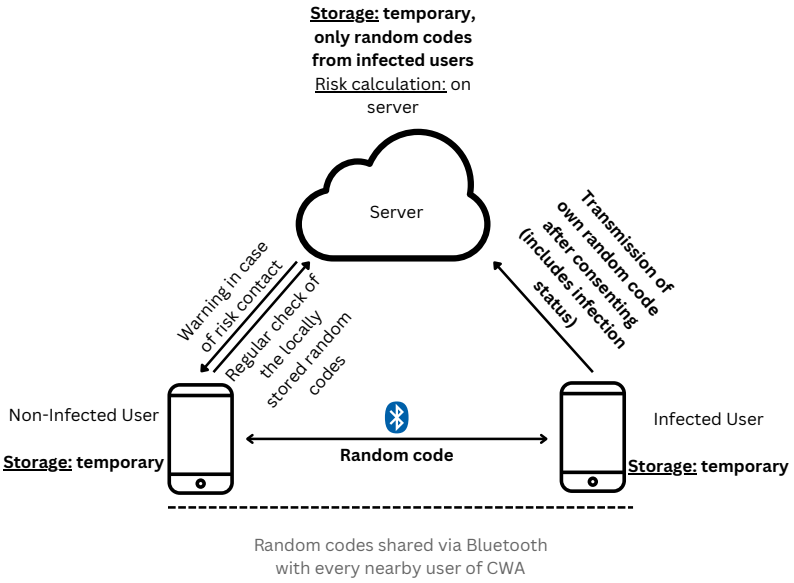


FIGURE C.2: Advanced technical mental model (n = 3, all users). The model is close to the correct functioning of the CWA, but participants assumed that the risk calculation is executed on the server. Bold text represents correct functionality.

Second Model: Simplified Model Three users and two non-users had a more simplified mental model (see Figure C.3). It is distinguished from the advanced technical model by the fact that participants possessed a basic understanding of the technical functionality but had less in-depth technical knowledge and more

misconceptions about data transmission. For example, it was assumed that contact information was captured using location data via Bluetooth, GPS, or both, with only Bluetooth being correct. Furthermore, participants with this mental model incorrectly thought that data transmission was the same for uninfected and infected users and that location data were transmitted from the smartphone to a server when contact was made with other users.

Participants with this mental model had mixed beliefs regarding data protection. Both users and non-users stated that the data was either anonymous (correct) or that the random codes could be matched to demographic data incorrect. The latter was expressed by the fact that participants assumed that parties they believed were involved (such as SAP, Telekom, health authorities, or the RKI) could access the data stored on the server (location data of all users, infection state and demographic data of infected users). Some also incorrectly thought that if the positive infection status was passed on voluntarily, other data such as one's name, address, date of birth, e-mail address, cell phone identification code, IP address, or app usage data would also be transmitted. One current user and another former user expressed feelings of ambiguity about the data entered during app installation, e.g., user4:*"Regarding the random numbers, of course, it has to be said that they have to be connected to my personal data somehow. Did I sign up for the COVID-19 app? I don't know at all. Do you have to register?"*

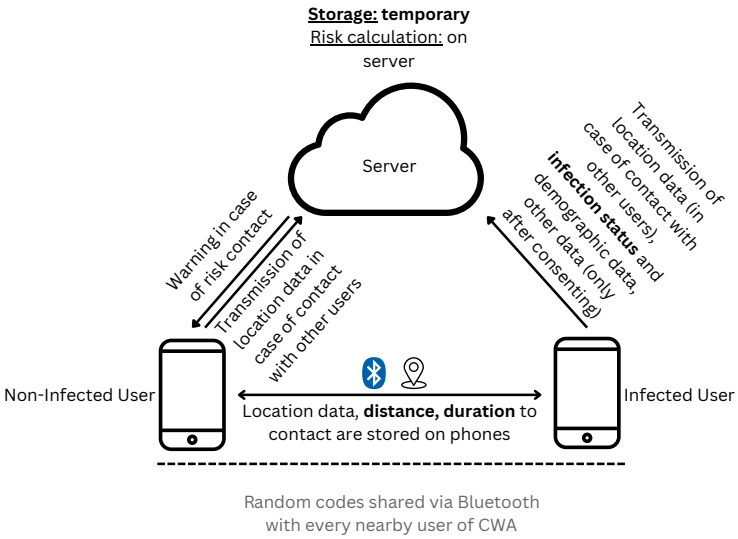


FIGURE C.3: The figure shows the simplified mental model extracted from the interviews (n = 5, three users and two non-users). It is characterized by few technical details and misconceptions about data transmission. The bold text represents correct functionality.

Third Model: Server Model Six non-users and three CWA users held the server model (see Figure C.4). Participants with this mental model had several incorrect assumptions: they believed that all data is transmitted via a server, and there is no direct data exchange between the smartphones of the CWA users. Additionally, they incorrectly assumed that information about encounters is captured solely through GPS data. Participants with this mental model thought that demographic data would be collected if a positive infection status was shared, with some participants assuming that this was mandatory and would be done automatically, with both assumptions being wrong. Most participants incorrectly thought that collected data would be stored on the server permanently. Four participants assumed that data from non-infected individuals would never be stored. Aside from storage, similar to the simplified model, the data transfer from infected and uninfected users to the server was assumed to be identical. The assessment of data protection as well as access to the server was also similar to that of the simplified model. Notable in this model was the misconception by four participants that notifications of a risk encounter would occur immediately upon contact. This could be due to the fact that two non-users and one user thought that the CWA would work like Google Maps, e.g., user7: *"In the end it is like Google Maps. That's kind of how I imagine it. Everybody who uses the Warnapp is listed in Google Maps and then you just see who's near who and who's infected and who's not infected."* Additionally, three participants incorrectly believed that the CWA would protect against infection by warning users prior to a potential contact with an infected person.

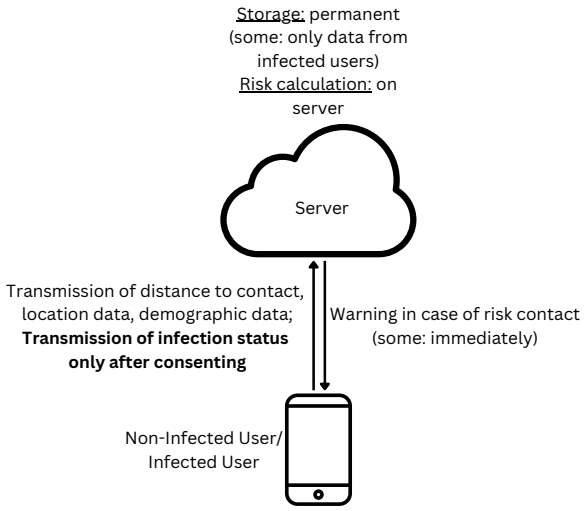


FIGURE C.4: The figure shows the server mental model extracted from the interviews (n = 9, three users and six non-users). The key point is that the participants thought that all data was transmitted via a server. The bold text represents correct functionality.

Fourth Model: Local Model Three participants (two non-users and one user) had a mental model without a server (see Figure C.5). Similar to the simplified model, participants with this mental model believed that contact tracing was done via Bluetooth, GPS, or both (with only Bluetooth being correct). Consistent with the idea of a missing server, participants correctly thought that the data collected would be stored locally and temporarily on the smartphones of the users, which also meant that the risk calculation was carried out locally. In the course of the interviews, it became apparent that the participants were unsure about how the data exchange worked. This was shown, e.g., by a non-user who did not consider that a risk encounter could also occur by sharing a positive test after the contact encounter. One user was aware that a risk encounter could also be defined as such retrospectively if a positive test was shared after the encounter had already taken place but could not explain where the CWA could get the information about this retrospectively shared positive test from. Another non-user stated concerns about the vendors' misuse of location data at the beginning of the interview. However, later in the interview, the same person described local data processing exclusively via Bluetooth and stated that access by manufacturers was impossible in their mental model. For example, nonuser5 stated:*"I always thought of it as just sharing location data, but since I don't need the location for the CWA, it can't be. Oh my gosh, I have no idea about that."* These inconsistencies in their own considerations indicate that some of the participants were not aware of or did not question the inconsistencies in their thinking of how the CWA works. This became evident when they were confronted with such questions.

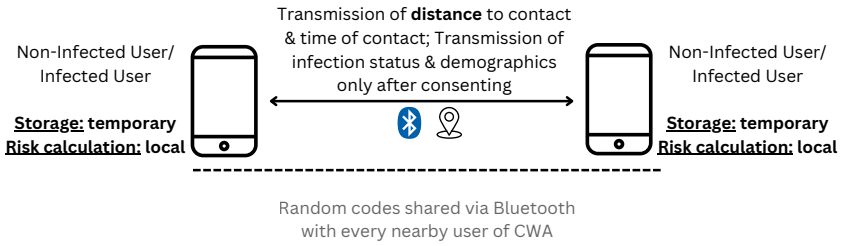


FIGURE C.5: The figure presents the local mental model (n = 3, one user and two non-users) extracted from the interviews. Here, all data is transferred directly from smartphone to smartphone without a server via which positive tests are shared.

Do the mental models of users and non-users differ? Although the sample of our interview study is too small to make reliable judgments about the systematic effect of app usage on mental models (RQ2) – we will address this question further in the consecutive survey study – the interviews suggest that users may

	Correct	**Advanced (n=3)**	**Simplified (n=5)**	**Server (n=9)**	**Local (n=3)**
CWA **user**?	-	yes=3, no=0	yes=3, no=2	yes=3, no=6	yes=1, no=2
Privacy was **important** for participants?	-	yes=2, no=1	yes=3, no=2	yes=4, no=5	yes=1, no=2
Storage on server	Temporary	Temporary	Temporary	Permanent	-
Storage on phone	Temporary	Temporary	Temporary	-	Temporary
Risk calculation	On phone	On server	On server	On server	On phone
Technology for encounter detection	Bluetooth	Bluetooth	Bluetooth or GPS	GPS	Bluetooth or GPS
Data transmitted to server	Own random codes incl. infection status *,**	Own random codes incl. infection status*,**	Location (in case of encounters), infection status*,**, demographic data *,**, other data*,**	Location, distance, demographic data, infection status*	-
Data transmitted between phones	Random codes	Random codes	Location, distance, duration	-	Distance, time, infection status*, demographic data*

TABLE C.7: The table summarizes the interviews' results. The four mental models based on participants' answers are compared to the correct model. Markings: *only with the user's consent, **only for infected users

be more likely to have mental models that correspond to the actual functioning of the CWA than non-users: all three participants who held the advanced technical model were users, and three additional users had the simplified but still roughly correct mental model of the CWA data collection and processing. Regarding the non-user participants, only two had a simplified mental model, whereas the remaining either had a server (6) or local (2) mental model.

However, four user participants also had a severely erroneous mental model of the app functioning (three *server*, one *local* mental model). Therefore, we cannot attribute a different understanding only to the usage status (or, conversely, the decision for or against app usage only to the technically correct understanding). This is also reflected in the responses to our explanation of how the CWA works: although six non-users commented positively on the knowledge gained through our explanation of how the app works, only two of them stated that they would reconsider their intention to use the app. When we asked the non-users again by email two weeks after the interview for their installation status, none of them reported currently using the CWA or intended to do so in the future. We will, thus, consider additional influencing factors in the next section.

The role of privacy, security and utility Our results suggest that users and non-users differ mainly in what benefits they see in the app: nine of the 10 non-users interviewed reported that the app's usefulness in the pandemic response was not really clear to them, while none of the users reported such doubts. All users stated that the app warns others and thus makes an important contribution to protecting the general public, while only half of the non-users spoke of protecting the general public as a goal of the app.

Still, privacy was an important factor for half of the participants in deciding whether or not to install the app. The well-implemented protection of their data was a pro argument for six users, while four non-users decided against installing

the app due to privacy concerns. Similarly, for four users and six non-users, data protection did not play a relevant role in the decision for or against the app.

Four participants (three users, one non-user) assumed that the app's program code would be open source, while eight participants (three users, five non-users) thought it would not be publicly available, and the others remained undecided on this front. Those who thought the code would not be open source considered open source to be fundamentally insecure, as the publicly available code could be used to exploit security vulnerabilities, access data, manipulate the app, or distribute a malicious copy of the app.

Interview Guide

Introduction:
Welcome and thank you for participating in the study. Today, as was mentioned in the consent form, we are talking about the Corona-Warn-App. The interview will last about 55 minutes and at the end, there is a questionnaire of about 5 minutes. Have you submitted the consent form? With this, I would then begin recording the conversation. Before we begin, I just wanted to say that today we'll probably touch on topics that you may not be very familiar with - but please do not worry, this is not a test. Rather, we are interested in how you think and feel: so there is no right and no wrong. If you think you do not know the answer to a question, just guess to the best of your ability. If ever a question is incomprehensible, please let me know, and I will try to explain or rephrase it. I would just like to point out to you again that this interview is voluntary, and you always have the option not to answer a question or to end the interview. If you have no other questions, I would start. [based on **Wu and Zappala** [226]]

Reasons for use/non-use and media

1. To start, I would like to get a sense of how you learned about the CWA and would therefore like to know:
   a. How did you find out about the CWA?
   b. What was your opinion of the app as a result?
2. Do you use the CWA?
   If no:
   i. Have you used the app before? Why did you uninstall the app?
   ii. Are you able to use the app? Can others help you to overcome the problems of using the Corona-Warn-App?
   If yes:
   i. How long have you been using the app?
3. I am now curious about what lies behind it: What reasons do you have for it?
   If used only after release:
   i. What convinced you?
   a. What other factors are there that influence your use of the app?
   b. What is the deciding factor for you to use/not use the app?
4. Now, I would like to ask some questions regarding the providers of the app.

a. Can you think of who the vendors of the CWA are?

b. Clarification: Just for the sake of completeness: The app is published by the Robert Koch Institute (RKI), and it was developed on behalf of the German federal government by the companies SAP and Deutsche Telekom AG, with the participation of around 25 other companies.

c. How trustworthy do you rate the developers, i.e., SAP and Deutsche Telekom with regard to your privacy protection? On a scale of 1 - 7, where 7 is the maximum, i.e., very trustworthy. (Why exactly this number?)

d. How trustworthy do you rate the federal government in terms of your privacy protection? On a scale of 1 - 7, where 7 represents the maximum - i.e., very trustworthy. (Why this exact number?)

e. How trustworthy do you rate the health departments in terms of your privacy protection? On a scale of 1 - 7, where 7 represents the maximum - i.e., very trustworthy. (Why this exact number?)

f. How would your trust in the vendor be if the app had been developed by private companies without government involvement?

g. What other factors influence how much you trust the CWA to store your data securely?

h. To what extent is your use of the CWA dependent on your trust in the privacy of the app?

5. How much do you trust the app to store your data securely and protect your privacy?

a. Regardless of the app, does sharing your health data worry you?
If yes:

i. What concerns do you have about sharing your health data?

ii. Did these concerns factor into your decision to use the app?

Knowledge and understanding of the functionality
Now I would like to start with the drawing task that I mentioned in the consent form. Before we begin, I want to remind you that this is not a test of your artistic skills; it's just to help me get a better feel for how you imagine things working. [based on **Wu and Zappala** [226]] At this point, I would ask you to say aloud any thoughts that come to you as you draw. Would you rather draw on the whiteboard or with pen and paper?

Now please imagine you have the CWA installed on your phone and you go shopping. While doing so, you pass by several people who also have the app installed. Could you please outline for me how the CWA works? That is, how

the data are stored, exchanged, and processed. Imagine the way it works and draw whatever that looks like. Take as much time as you need and let me know when you're done.
[Explanation of drawing tools.]
(Reference Think Aloud) Please speak your thoughts out loud.
(If drawing by hand) Could you take a picture of the drawing with your phone and email it to me? Thank you.
(If this is not possible) Could you briefly hold the picture up to your camera?

Regarding the drawing of the participant:

1. What data are collected?
2. Where will the data be stored?
   If an encrypted randomized key is mentioned:
   i. What is the function of the key?
   ii. How is the key generated?
   iii. How does the key exchange work?
3. Where do you think someone might have access or not have access to the data?
   a. Who has access to the data?
   b. How likely is such access?
   c. What would be the consequences of such access?
4. Imagine you are not infected and you pass by an uninfected person, where are your data processed?
   If decentralized data processing is mentioned:
   i. What does decentralized data processing mean in your own words?
5. Imagine you are not infected and you pass an infected person, where are your data processed?
6. Is the program code of the CWA publicly available?
   If open source is mentioned:
   i. What does open source mean?
   a. Would it make a difference to the security of your data if the program code was public?
7. What happens in the CWA if you were corona positive?
   a. What data are collected?

b. Where are the data processed?

c. Who has access to your data?

d. What consequences would this have for you?

8. How do you think the risk is calculated?

Clarification and repeat questions about app providers

At this point, I would like to summarize again how the CWA works in detail. The encounter recording runs in the background via Bluetooth Low Energy.

Whenever you encounter another person who is also using the app, the smartphones automatically exchange encrypted random codes. These random codes only contain data about the fact that two people met, how long this lasted, and how big the distance was. No conclusions about your identity or your location are possible. The random codes change every 24 hours and are stored on your smartphone for 14 days. The period of 14 days was chosen because an infected person is not contagious for more than 14 days. If a user is proven to be infected, they can voluntarily provide their random codes anonymously to other users. To prevent misuse, a positive test result must be verified via a QR code or teleTan, which they must be provided when collecting the test sample. If the user decides to inform others, their own daily keys of the last 14 days are transmitted to the server. The server transmits the random codes to all other users. Here you have to distinguish 3 cases:
- 1. If you are tested positive, your tag key will only be sent to the server if you agree.
- 2. If a passer-by is tested positive, their tag key will only be sent to the server if they agree.
- 3. If no one tests positive, no key will be sent to the server.

In any case, however, the tag keys are exchanged between the passers-by. The risk calculation is then performed on the smartphone of the user. **Depending on the risk assessment, the app displays a low or increased risk, including a recommendation for action**. This procedure corresponds to decentralized data processing. Furthermore, the program code of the CWA is publicly available. Do you have any questions in this regard, or is something unclear?

Now, in relation to your previous explanation, I would like to repeat some questions.

1. Trustworthiness of providers

   a. How trustworthy do you rate the developers, i.e., SAP and Deutsche Telekom in terms of their privacy protection? On a scale of 1 - 7, where 7 represents the maximum - i.e., very trustworthy. (Why does this differ from the rating at the beginning of the interview?)
   b. How trustworthy do you rate the federal government in terms of its protection of your privacy? On a scale of 1 - 7, with 7 being the maximum - very trustworthy. (Why is this different from the rating at the beginning of the interview?)
   c. How trustworthy do you rate health departments in terms of their privacy protections? On a scale of 1 - 7, with 7 representing the maximum - i.e., very trustworthy. (Why is this different from the rating at the beginning of the interview?)
   d. How much do you trust the app to store your data securely and keep your privacy protected?

2. Why do you think the government has decided to decentralize data processing?

3. Why do you think the government has decided to make the program code of the CWA publicly available?

4. Do you use other apps, such as messenger or navigation apps that use similarly sensitive data as the CWA?

   a. How trustworthy do you rate the providers of these apps?
   b. Does trustworthiness in the provider play a role for or against using these apps?

5. As of April 2021, the CWA includes event registration functionality. This allows users to register at retail, events, or private meetings and check in via QR code. Potential clusters can thus be identified and chains of infection can be interrupted in a targeted manner.

   a. How has this affected your privacy?
   b. How has this functionality affected your usage patterns regarding the app?

6. If non-users:

   a. Do you now intend to use the CWA?
   b. Under what conditions would you use the app?

Optional questions about covariates

We are now almost at the end of the interview and I would now like to ask you a few more questions, but you do not have to answer them if you feel uncomfortable doing so.

1. To the best of your knowledge, is there a person in your personal environment who belongs to a risk group?
2. Is there a person in your personal environment who is or has been tested positive for Covid-19?
3. Are you or have you been tested positive for Covid-19?
4. (Did any of these three factors play a role in your decision to use the app?)

This brings us to the end of the interview and I would now end the recording. I would then ask you to answer a short 5-minute questionnaire at the following link, after which you are welcome to give me your bank account details for the transfer of the remuneration.

[Request bank account data]

We have now reached the end.

1. Is there anything else you would like to say at this point?
2. Do you have any questions or comments?
3. Now I would like to tell you about the research questions of this study: First, we want to find out what mental models users and non-users of the CWA have about how it works and to what extent these models influence the decision to use it. Furthermore, we want to discuss factors that lead to more trust in such an application to improve the development and marketing of future applications that process sensitive data.

Thank you for participating in this study.

Interview Codebook

Theme	Category	Code	N
Incorrect Assumptions	Collected data	Location data	12
		Demographic data	9
		Cell phone model	1
		Data entered when installing the CWA	1
		Further data	2
	Data storage	No storage of data if not infected	4
		Always central storage of the data	11
	Data transmission	Notification about contact immediately	3
		No different data transmission infected/not infected	6
		Contact of users identifiable	1
		Satellite transmission	3
		WLAN data transmission	1
		Test result is recorded in app without consent	3
	Data processing	Data processing on server	4
		Ambiguity about risk calculation	5
	Accessibility of data	German government	6
		Third parties	2
		Health Department	3
		SAP	1
		Telekom	1
	App features	CWA protects against infection	1
		CWA works like Google Maps/all users visible	3
	Open source is more insecure	Copy of the app through open source	3
		Manipulation of the app through open source	3
		Exploit security vulnerabilities through open source	5
		Access to data through open source	3
	Privacy concerns regarding CWA	Fear of surveillance	5
		Backdoors built in	3
		Bluetooth not reliable/insecure	1
		Data is collected anyway	2
		Data misuse by provider	3
		Deanonymization possible	2
		Hacker attack	6
		Location data is collected anyway	1
		Security gaps	4
		Doubts about data protection	6
	Benefit of the app	Serves for self-protection	1
		Vaccination makes app useless	2
		Information about infection useless after encounter	1
	Benefit of the app	No benefit since little contacts per se	7
		No benefit, because too few people use CWA	6
		Unsure about the benefits of the app	7
Correct Assumptions	Collected data	Distance to contact	7
		Contact duration	5
		Infection status	12
		IP address	1
		Time of contact	3
	Data storage	Decentralized storage	1
		Local storage	5
		Temporary storage	6
	Data transmission	Notification about contact time-delayed	10
		Bluetooth	4
		Infection data transmission only after consent	13
		Only data of the infected is transferred to the server	4
		Server / Cloud / Central for data transmission	4
		Transfer between smartphones	8
		Verification of the infection status	2
		Random code / encryption	7
	Data processing	Data anonymous	7
		Knowledge about risk calculation	3
		Risk calculation on the cell phone	1
	Benefit of the app	Warn others	2
		Breaking chains of infection	3
		Protection of the general public	11
		Be warned yourself	5
	Program code public	Not public	8
		Public	4
	Developers/manufacturers/providers	RKI	0
		Telekom	3
		SAP	6
		German government	12

TABLE C.8: Codebook used for the interview study

Appendix D

Appendix for "Can Johnny be a whistleblower"

D.1 Study Material

Scenario

This are the (translated) scenario texts available to the participants, including the payment description for both studies.

Scenario Text for Study 1 (Translated)

The study consists of a role play in which you take on the role of Alex. The scenario is described in the following text. Please read the text carefully and put yourself in the situation.

Scenario card Your name is Alex and you live in a country ruled by an authoritarian regime. Both blanket and targeted surveillance is a daily phenomenon. You work in a high-ranking government agency. A colleague, Hannah, has gained access to extremely sensitive information about high-level corruption and shared it with you in encrypted form through the Signal app a few months ago. This information includes revelations about illegal activities by politicians.

You want this information to be made public. In order to avoid drawing suspicion to Hannah, who had access to the data, you have decided to wait a few months and then send the data to journalists. The time has now come and you can begin.

You already have business cards from three trustworthy investigative journalists from abroad. You have received them personally and you trust the information on them. All journalists are known for their integrity and have already uncovered a number of major scandals. All three journalists offer whistleblowers that they can be contacted securely via the Signal app.

You have a rough idea of how such a contact works: First you send the data to the journalist. The journalist then does research and checks whether the data is genuine. Once they are satisfied, they publish the story. This can take a while.

The archive containing the data and explanation can be found in your Signal app in the chat with Hannah. You are familiar with the content and the exact content does not matter for the study.

Your goal is to ensure that all three journalists receive the data about the corruption. Considering the dangers you and Hannah face if your government's intelligence agencies find out that you have leaked the data, it is crucial for you to make sure that you communicate with the journalists in encrypted form using the Signal app. You are sure that as long as you use the Signal app correctly, the secret services will not be powerful enough to break the encryption or access the metadata.

Bonus payment: You currently have €5 in your account. For every journalist you successfully send the data to, you will receive another €5. However, if you are caught by the secret service, you will end up in prison and will not receive any payment. So only send the data if you are sure that the Signal app will protect you. You will receive the exam bonus of 2% points even if you end up in prison. If you are not caught, you will receive the 2% points and the money from your account.

Instructions

Signal Signal is an encrypted messenger and phone app. Signal saves your number, but does not create a log file for your incoming or outgoing communication. Signal is easy to use: Open the app and tap the pencil icon (bottom right on Android phones) to write a new message. Enter the desired phone number in the search field. You can now send an encrypted message via Signal.

How do I take screenshots? Press and hold the "On/Off" button and "Volume down" button on your phone at the same time for about one second.

Scenario Text for Study 1 (Original)

Die Studie besteht aus einem Rollenspiel in dem du die Rolle von Alex einnimmst. Im folgenden Text wird das Szenario beschrieben. Bitte lies den Text aufmerksam durch und versetze dich in die Situation.

Szenarienkarte Du heißt Alex und wohnst in einem Land das von einem autoritärem Regime regiert wird. Sowohl flächendeckende wie auch gezielte Überwachung ist ein tägliches Phänomen. Du arbeitest in einer hochrangigen Regierungsbehörde. Eine Kollegin, Hannah, hat Zugang zu äußerst sensiblen Informationen über Korruption auf höchster Ebene erhalten und vor ein paar Monaten verschlüsselt durch die Signal App mit dir geteilt. Diese Informationen enthalten u.a. Enthüllungen über illegale Aktivitäten von Politikern. Ihr wollt, dass diese Informationen veröffentlicht werden. Um möglichst keinen Verdacht auf Hannah zu lenken, die Zugriff auf die Daten hatte, habt ihr beschlossen, dass du ein paar Monate wartest und dann die Daten an JournalistInnen schickst. Die Zeit ist jetzt gekommen und du kannst beginnen.

Du hast bereits Visitenkarten von drei vertrauenswürdigen InvestigativjournalistInnen aus dem Ausland. Diese hast du persönlich erhalten und du vertraust den Informationen die darauf stehen. Alle JournalistInnen sind für ihre Integrität bekannt und haben bereits eine Reihe von bedeutenden Skandalen aufgedeckt. Alle drei JournalistInnen bieten WhistleblowerInnen an, dass sie über die Signal App sicher kontaktiert werden können.

Du hast eine ungefähre Vorstellung wie so ein Kontakt abläuft: Erst schickst du dem/der JournalistIn die Daten. Diese/r recherchiert dann und prüft ob die Daten echt sind. Wenn sie sich davon überzeugt hat, veröffentlicht sie die Geschichte. Das kann eine Weile dauern. Das Archiv, das die Daten und Erklärung enthält befindet sich in deiner Signal App im Chat mit Hannah. Du bist mit dem Inhalt vertraut und der genaue Inhalt spielt für die Studie keine Rolle.

Dein Ziel ist es, dass alle drei JournalistInnen die Daten über die Korruption erhalten. In Anbetracht der Gefahren, die dir und Hannah drohen, falls die Geheimdienste deiner Regierung rausfinden, dass du die Daten geleakt hast, ist es für dich von entscheidender Bedeutung, sicherzustellen, dass du mit den JournalistInnen verschlüsselt mit der Signal App kommunizierst. Du bist dir sicher, dass solange du die Signal App korrekt nutzt, die Geheimdienste nicht mächtig genug sind die Verschlüsselung zu brechen oder an die Meta-daten zu gelangen.

Bonuszahlung: Du hast aktuell 5 €auf deinem Konto. Für jede/n JournalistIn der/dem du erfolgreich die Daten schickst, erhältst du weitere 5 €. Solltest du allerdings vom Geheimdienst erwischt werden, landest du im Gefängnis und bekommst keine Auszahlung. Verschicke die Daten also nur wenn du dir sicher bist, dass die Signal App dich schützt. Den Klausurbonus von 2% Punkten erhältst du auch wenn du im Gefängnis landest. Wenn du nicht erwischt wirst, erhältst du die 2% Punkte und das Geld von deinem Konto.

Anleitungen

Signal Signal ist ein verschlüsselter Messenger und eine Telefon-App. Signal speichert deine Nummer, legt aber keine Logdatei zu deiner ein- oder ausgehenden Kommunikation an. Signal ist einfach zu bedienen: Öffne die App und tippe auf das Stift-Symbol (bei Android-Handys unten rechts), um eine neue Nachricht zu schreiben. Gib die gewünschte Telefonnummer in das Suchfeld ein. Schon kannst du eine verschlüsselte Nachricht per Signal versenden.

Wie mache ich Screenshots? Halte die "Ein/Aus"-Taste und "Leiser"-Taste des Handys gleichzeitig für etwa eine Sekunde gedrückt.

Scenario Text for Study 2 (Translated)

The study consists of a role play in which you take on the role of Alex. The scenario is described in the following text. Please read the text carefully and put yourself in the situation.

Scenario Description

Your name is Alex and you live in a country ruled by an authoritarian regime.

Both blanket and targeted surveillance happen on a daily basis. You work in a high-ranking government agency. A colleague, Hannah, has gained access to extremely sensitive information about high-level corruption and shared it with you in encrypted form through the Signal app a few months ago. This information includes revelations about illegal activities by politicians. You want this information to be made public. In order to avoid drawing suspicion to Hannah, who had access to the data, you have decided that you will wait a few months and then you (Alex) will send the data to journalists. The time has now come and you can begin.

You already have business cards from three trustworthy investigative journalists from abroad. You have received the business cards personally from the journalists and you trust the information on them. All journalists are known for their integrity and have already uncovered a number of major scandals. All three journalists offer whistleblowers that they can be contacted securely via the Signal app.

You have a rough idea of how such a contact works: First you send the data to the journalist. The journalist then researches and checks whether the data is genuine. If the journalist is convinced, the story is published. This can take a while. The archive containing the data and explanation can be found in your Signal app in the chat with Hannah. They are familiar with the content but the exact content does not matter for the study.

Your goal is for all three journalists to receive the data on corruption. Considering the dangers you and Hannah face if your government's intelligence services find out that you have leaked the data, it is crucial for you to ensure that you communicate with the journalists in encrypted form using the Signal app. You are sure that as long as you use the Signal app correctly, the intelligence services will not be able to break the encryption or access the metadata.

Payment: You will receive a basic payment of €15 after completing the study. You also have the option of receiving a bonus of up to €9.

You should send the data to the journalists with a secure connection - and only to those with a secure connection.

A decision must be made for each of the three journalists individually:
- If the connection is secure, the data must be sent.
- If the connection is insecure, no data may be sent.

For each correct decision you receive a €3 bonus, i.e. up to €9 in total. But: No bonus is awarded, - if data is sent via at least one insecure connection
- or if no data is sent although there is at least one secure connection.

How to send messages with Signal
Open the app and tap the pencil icon at the bottom right to write a new message. Enter the desired phone number in the search field. You can now send an encrypted message via Signal.

What is a secure connection?
The Signal app offers you methods to ensure that you are communicating with

the right person and correctly encrypted. If you cannot use the app to ensure that the connection is secure, you should assume that the connection is insecure.

Scenario Text for Study 2 (Original)

Die Studie besteht aus einem Rollenspiel in dem Sie die Rolle von Alex einnehmen. Im folgenden Text wird das Szenario beschrieben. Bitte lesen Sie den Text aufmerksam durch und versetzen sich in die Situation. **Szenarienbeschreibung**
Sie heißen Alex und wohnen in einem Land, das von einem autoritären Regime regiert wird. Sowohl flächendeckende als auch gezielte Überwachung passiert täglich. Sie arbeiten in einer hochrangigen Regierungsbehörde. Eine Kollegin, Hannah, hat Zugang zu äußerst sensiblen Informationen über Korruption auf höchster Ebene erhalten und vor ein paar Monaten verschlüsselt durch die Signal App mit dir geteilt. Diese Informationen enthalten u.a. Enthüllungen über illegale Aktivitäten von Politikern. Ihr wollt, dass diese Informationen veröffentlicht werden. Um möglichst keinen Verdacht auf Hannah zu lenken, die Zugriff auf die Daten hatte, habt ihr beschlossen, dass ihr ein paar Monate wartet und Sie (Alex) dann die Daten an JournalistInnen schicken. Die Zeit ist jetzt gekommen und Sie können beginnen.

Sie haben bereits Visitenkarten von drei vertrauenswürdigen InvestigativjournalistInnen aus dem Ausland. Die Visitenkarten haben Sie persönlich von den JournalistInnen erhalten und Sie vertrauen den Informationen, die darauf stehen. Alle JournalistInnen sind für ihre Integrität bekannt und haben bereits eine Reihe von bedeutenden Skandalen aufgedeckt. Alle drei JournalistInnen bieten WhistleblowerInnen an, dass sie über die Signal App sicher kontaktiert werden können.

Sie haben eine ungefähre Vorstellung wie so ein Kontakt abläuft: Erst schicken Sie dem/der JournalistIn die Daten. Diese/r recherchiert dann und prüft, ob die Daten echt sind. Wenn der/die JournalistIn davon überzeugt ist, wird die Geschichte veröffentlicht. Das kann eine Weile dauern. Das Archiv, das die Daten und Erklärung enthält, befinden sich in ihrer Signal App im Chat mit Hannah. Sie sind mit dem Inhalt vertraut aber der genaue Inhalt spielt für die Studie keine Rolle.

Ihr Ziel ist es, dass alle drei JournalistInnen die Daten über die Korruption erhalten. In Anbetracht der Gefahren, die Ihnen und Hannah drohen, falls die Geheimdienste eurer Regierung herausfinden, dass Sie die Daten geleakt haben, ist es für Sie von entscheidender Bedeutung, sicherzustellen, dass Sie mit den JournalistInnen verschlüsselt mit der Signal App kommunizierst. Sie sind sich sicher, dass solange Sie die Signal App korrekt nutzt, die Geheimdienste nicht in der Lage sind die Verschlüsselung zu brechen oder an die Metadaten zu gelangen.

Zahlung: Sie erhalten eine Basiszahlung von 15 € nach Abschluss der Studie. Zusätzlich haben Sie die Möglichkeit, bis zu 9 € Bonus zu erhalten.

Sie sollen die Daten an die JournalistInnen mit einer sicheren Verbindung schicken – und zwar nur an diejenigen mit einer sicheren Verbindung.

Für jeden/jede der drei JournalistInnen muss einzeln entschieden werden:
– Ist die Verbindung sicher, so müssen die Daten geschickt werden.
– Ist die Verbindung unsicher, so dürfen keine Daten geschickt werden.

Für jede richtige Entscheidung erhalten Sie 3 € Bonus, also insgesamt bis zu 9 €. Aber: Es entfällt jeglicher Bonus,
– wenn Daten über mindestens eine unsichere Verbindung gesendet werden,
– oder, wenn keine Daten gesendet werden, obwohl es mindestens eine sichere Verbindung gibt.

Wie verschickt man Nachrichten mit Signal?
Öffnen Sie die App und tippen Sie auf das Stift-Symbol unten rechts, um eine neue Nachricht zu schreiben. Geben Sie die gewünschte Telefonnummer in das Suchfeld ein. Schon können Sie eine verschlüsselte Nachricht per Signal versenden.

Was ist eine sichere Verbindung?
Die Signal-App bietet Ihnen Methoden an, um sicherzustellen, dass Sie mit der richtigen Person und korrekt verschlüsselt kommunizieren. Wenn Sie mit der App nicht sicherstellen können, dass die Verbindung sicher ist, sollten Sie davon ausgehen, dass die Verbindung unsicher ist.

Survey (Including Translation)

The survey varied slightly in the first and the second study. Social authentication was called "Proof of identity (Identitätsnachweis)" in the second study and participants were addressed more formally. The questions that were exclusively part of a study or edited a lot are marked. The original text was in German, we provide here a translated version.

Q1: Im Folgenden stellen wir einige Fragen zu den Methoden mit denen du während der Studie interagiert hast. Die Laborstudie enthält ein Rollenspiel. Bitte fülle aber diesen Fragebogen nicht in der Rolle als Alex aus, sondern als du selbst. (Type: Text)

Q1: Below are some questions about the methods you interacted with during the study. The lab study includes a role play. However, please do not fill out this questionnaire in the role of Alex, but as yourself. (Type: Text)

Q2: Bitte gib dein Studienpseudonym ein (Type: Text Entry)

Q2: Please enter your study pseudonym (Type: Text Entry)

Q3: Verwendest du, unabhängig von der Studie, die Signal App? (Type: MC)
Antwortoptionen: *"Nein."*, *"Ja, selten"*, *"Ja, häufig"*

Q3: Do you use the Signal app independently of the study? (Type: MC)
Answer Choices: *"No", "Yes, Rarely", "Yes, Often"*

Q4: Bevor du an der Studie teilgenommen hast: Bei wie vielen deiner Chat-Kontakte hast du eine Sicherheitsnummer (z.B. in Whatsapp oder Signal) verwendet, um den Kontakt zu verifizieren? (Type: MC)
Antwortoptionen: *"Bei keinem meiner Chat-Kontakte.", "Bei einigen meiner Chat-Kontakte.", "Bei etwa der Hälfte meiner Chat-Kontakte.", "Bei den meisten meiner Chat-Kontakte.", "Bei nahezu allen meiner Chat-Kontakte."*

Q4: Before you took part in the study: For how many of your chat contacts did you use a safety number (e.g. in Whatsapp or Signal) to verify the contact? (Type: MC)
Answer Choices: *"With none of my chat contacts", "With some of my chat contacts", "With about half of my chat contacts", "With most of my chat contacts", "With almost all of my chat contacts".*

Q5: Während der Studie hast du bis zu drei verschiedene Methoden ausgetestet wie man einen Kontakt über Signal verifizieren kann. a) per QR-Code Scan b) den Vergleich von Sicherheitsnummern c) über Accountzugehörigkeit auf Platformen (Social Authentication)In den folgenden Fragen geht es um deine Gedanken bezüglich genau dieser Methoden. (Type: Text)

Q5: During the study, you tested up to three different methods of verifying a contact via Signal. a) via QR code scan b) comparing safety numbers c) via account affiliation on platforms (social authentication). The following questions are about your thoughts on exactly these methods. (Type: Text)

Q6: Welche der Methoden hast du angewendet im Verlauf der Studie? (Type: MC)
Antwortoptionen: *"QR-Code", "Sicherheitsnummer", "Social Authentication"*

Q6: Which of the methods did you use in the course of the study? (Type: MC)
Answer Choices: *"QR code", "safety number", "social authentication"*

Q7: Wie sehr stimmst du der folgenden Aussage zu: Ich habe Vertrauen in diese Methode zur Verifizierung der Sicherheitsnummern in Signal. *Study2: Ich habe Vertrauen in diese Methode zur Überprüfung der Identität meiner GesprächspartnerInnen.* (Type: Matrix)
Items: *"Sicherheitsnummer", "Social Authentication", "QR-Code"*
Scale (5): *Stimme überhaupt nicht zu, Stimme eher nicht zu, Weder zustimmen noch ablehnen/neutral, Stimme eher zu, Stimme voll und ganz zu*

Q7: How much do you agree with the following statement: I have confidence in this method of verifying safety numbers in Signal. *Study2: I have confidence in this method for verifying the identity of my conversation partners.* (Type: Matrix)
Items: *"safety number", "social authentication", "QR code"*

Scale (5): *Strongly disagree, Somewhat disagree, Neither agree nor disagree/neutral, Somewhat agree, Strongly agree*

Q8: Wie sehr stimmst du der folgenden Aussage zu: Ich bin mir sicher, dass ich beim Verwenden der Methode die richtige Entscheidung getroffen habe. (Type: Matrix) Items: *"Sicherheitsnummer", "Social Authentication", "QR-Code"*
Scale (5): *Stimme überhaupt nicht zu, Stimme eher nicht zu, Weder zustimmen noch ablehnen/neutral, Stimme eher zu, Stimme voll und ganz zu*

Q8: How much do you agree with the following statement: I am sure that I made the right decision when using the method. (Type: Matrix)
Items: *"safety number", "social authentication", "QR code"*
Scale (5): *Strongly disagree, Somewhat disagree, Neither agree nor disagree/neutral, Somewhat agree, Strongly agree*

Q9: Bezogen auf das Verifizieren mit der entsprechenden Methode: Insgesamt, wie schwierig oder einfach war es, die Aufgabe abzuschließen? *Study 2: Bezogen auf das Überprüfen der Identität mit der entsprechenden Methode: Wie fanden Sie es die Aufgabe abzuschließen?* (Type: Matrix)
Items: *"Sicherheitsnummer", "Social Authentication", "QR-Code"*
Scale (5): *Sehr schwer, Sehr einfach*

Q9: In terms of verifying with the appropriate method: Overall, how difficult or easy was it to complete the task? *Study 2: Related to verifying identity using the appropriate method: How did you find completing the task* (Type: Matrix)
Items: *"safety number", "social authentication", "QR code"*
Scale (5): *Very difficult, Very easy*

only Study 2: Q10: Bitte markieren Sie welche Methode Sie wählen würden, wenn Sie eine/n Freund/in verifizieren müssten. (Type: MC) Items: *"Sicherheitsnummer", "Identitätsnachweise", "QR-Code"*

only Study 2: Q10: Please mark which method you would choose if you had to verify a friend. (Type: MC) Items: *"safety number", "social authentication", "QR code"*

Q11: Möchtest du uns bzgl. der Methoden sonst noch etwas mitteilen? (Type: Text Entry)

Q11: Is there anything else you would like to tell us about the methods? (Type: Text Entry)

Q12: Bitte geben Sie den Grad Ihrer Zustimmung zu folgenden Aussagen an. (Type: Matrix)
Items: *"Ich habe das Szenario verstanden.", "Ich halte das Szenario für plausibel.", "Ich habe mich in das Szenario reingedacht.", "Die Chance Geld zu bekommen hat*

mich motiviert möglichst viele Journalisten zu kontaktieren.", "Das Risiko Geld zu verlieren hat mich motiviert vorsichtig zu sein.", "Der finanzielle Anreiz hat mir geholfen mich in das Szenario einzufühlen.", "Ohne finanziellen Anreiz hätte ich das Szenario nicht so ernst genommen"., "Ohne finanziellen Anreiz hätte ich mir nicht so viel Mühe gegeben die Sicherheitsnummern zu überprüfen." Scale (5): *Stimme überhaupt nicht zu, Stimme eher nicht zu, Weder zustimmen noch ablehnen/neutral, Stimme eher zu, Stimme voll und ganz zu*

Q12: Please indicate your level of agreement with the following statements. (Type: Matrix)
Items: *"I understood the scenario", "I think the scenario is plausible", "I thought myself into the scenario", "The chance of getting money motivated me to contact as many journalists as possible", "The risk of losing money motivated me to be careful", The financial incentive helped me to empathize with the scenario", "Without a financial incentive I would not have taken the scenario so seriously", "Without a financial incentive I would not have gone to so much trouble to check the security numbers"*.
Scale (5): *Strongly disagree, Somewhat disagree, Neither agree nor disagree/neutral, Somewhat agree, Strongly agree*

Q13: Im Folgenden geht es um Ihre Interaktion mit technischen Systemen. Mit ‚technischen Systemen' sind sowohl Apps und andere Software-Anwendungen als auch komplette digitale Geräte (z.B. Handy, Computer, Fernseher, Auto-Navigation) gemeint. Bitte geben Sie den Grad Ihrer Zustimmung zu folgenden Aussagen an. (Type: Matrix)
Items: *"Ich beschäftige mich gern genauer mit technischen Systemen.", "Ich probiere gern die Funktionen neuer technischer Systeme aus.", "In erster Linie beschäftige ich mich mit technischen Systemen, weil ich muss.", "Wenn ich ein neues technisches System vor mir habe, probiere ich es intensiv aus.", "Ich verbringe sehr gern Zeit mit dem Kennenlernen eines neuen technischen Systems.", "Es genügt mir, dass ein technisches System funktioniert, mir ist es egal, wie oder warum", "Ich versuche zu verstehen, wie ein technisches System genau funktioniert.", "Es genügt mir, die Grundfunktionen eines technischen Systems zu kennen", "Ich versuche, die Möglichkeiten eines technischen Systems vollständig auszunutzen."*
Scale (6): *Stimmt gar nicht, Stimmt weitgehend nicht, Stimmt eher nicht, Stimmt eher, Stimmt weigehend, Stimmt völlig*

Q13: The following is about your interaction with technical systems. By 'technical systems' we mean apps and other software applications as well as complete digital devices (e.g. cell phone, computer, TV, car navigation). Please indicate your level of agreement with the following statements. (Type: Matrix)
Items: *"I like to take a closer look at technical systems", "I like to try out the functions of new technical systems", "I primarily deal with technical systems because I have to", "When I have a new technical system in front of me, I try it out intensively", "I like to spend a lot of time getting to know a new technical system", "It is enough for me that a technical system works, I don't care how or why", "I try to understand exactly*

how a technical system works", "It is enough for me to know the basic functions of a technical system", "I try to make full use of the possibilities of a technical system".
Scale (6): *Not true at all, Not true to a large extent, Rather not true, Rather true, Moderately true, Completely true*

Q14: Wie alt bist du? (Type: Text Entry)

Q14: How old are you? (Type: Text Entry)

only Study 2: Q15: Welchem Geschlecht fühlen Sie sich zugehörig? (Type: MC)
Antwortoptionen: *"Weiblich", "Männlich", "Divers", "Möchte ich selber beschreiben:", "Keine Angabe"*

only Study 2: Q15: Which gender do you feel you belong to? (Type: MC)
Answer Choices: *"Female", "Male", "Diverse", "I would like to describe myself:", "Not specified"*

only Study 2: Q16: Welche Erwerbssituation passt für Sie? Was in dieser Liste trifft auf Sie zu? Bitte beachten Sie, dass unter Erwerbstätigkeit jede bezahlte bzw. mit einem Einkommen verbundene Tätigkeit verstanden wird. (Type: MC)
Antwortoptionen: *"Vollzeiterwerbstätig", "Teilzeiterwerbstätig", "Altersteilzeit (unabhängig davon, ob in der Arbeits- oder Freistellungsphase befindlich)", "Geringfügig erwerbstätig, 450-Euro-Job, Minijob", "„Ein-Euro-Job" (bei Bezug von Arbeitslosengeld II)", "Gelegentlich oder unregelmäßig beschäftigt", "In einer beruflichen Ausbildung/Lehre", "In Umschulung", "Freiwilliger Wehrdienst", "Bundesfreiwilligendienst oder Freiwilliges Soziales Jahr", "Mutterschafts-, Erziehungsurlaub, Elternzeit oder sonstige Beurlaubung (bei Altersteilzeit die entsprechende Option anklicken)", "Nicht erwerbstätig (einschließlich: Schüler/-innen oder Studierende, die nicht gegen Geld arbeiten, Arbeitslose, Vorruheständler/-innen, Rentner/-innen ohne Nebenverdienst)"*

only Study 2: Q16: Which employment situation suits you? What in this list applies to you? Please note that gainful employment is understood to mean any paid or income-related activity associated with an income. (Type: MC)
Answer Choices: *"Full-time employment", "part-time employment", "partial retirement (regardless of whether in the working or release phase)", "marginally employed, 450-euro job, mini-job", ""one-euro job" (in receipt of unemployment benefit II)", "occasionally or irregularly employed", "In vocational training/apprenticeship", "In retraining", "Voluntary military service", "Federal voluntary service or voluntary social year", "Maternity leave, parental leave, parental leave or other leave of absence (click on the relevant option for partial retirement)", "Not gainfully employed (including: Pupils or students who do not work for money, unemployed, early retirees, pensioners without additional income)"*

only Study 2: Q17: Wenn Sie nicht vollzeit- oder teilzeiterwerbstätig sind: Sagen Sie bitte, zu welcher Gruppe auf dieser Liste Sie gehören. (Type: MC)

Antwortoptionen: *"Schüler/-innen an einer allgemeinbildenden Schule", "Studenten/-innen", "Rentner/-innen, Pensionäre/-innen, im Vorruhestand", "Arbeitslose", "Dauerhaft Erwerbsunfähige", "Hausfrauen/Hausmänner", "Sonstiges, und zwar:"*

*only Study 2:*Q17: If you are not in full-time or part-time employment: Please say, which group on this list you belong to. (Type: MC)
Answer Choices: *"Pupils at a general school", "students", "pensioners, retired, early retired", "unemployed", "permanently disabled", "housewives/househusbands", "other, namely:"*

Q18: Bitte beachte, dass es wichtig ist, dass die in diesem Fragebogen gestellten Fragen von jedem Teilnehmer unabhängig und ohne vorherige Kenntnis der Studie beantwortet werden. Dies gewährleistet die Integrität und Qualität unserer Daten. Wir bitten dich daher, keine Informationen über den Inhalt der Studie oder die Fragen dieses Fragebogens für 2 Wochen mit anderen Personen zu teilen.Deine Antwort auf die nächste Frage hat keinerlei Auswirkungen für dich, deine Bonuspunkte oder Bonuszahlung! Aber es ist für uns sehr wichtig das du ehrlich antwortest.Wusstest du bereits vor Teilnahme der Studie von Details was in der Studie passiert? *Study2:*Bitte beachten Sie, dass es wichtig ist, dass die in diesem Fragebogen gestellten Fragen von jedem Teilnehmer unabhängig und ohne vorherige Kenntnis der Studie beantwortet werden. Dies gewährleistet die Integrität und Qualität unserer Daten. Wir bitten Sie daher, keine Informationen über den Inhalt der Studie oder die Fragen dieses Fragebogens für eine Woche mit anderen Personen zu teilen. Ihre Antwort auf die nächste Frage hat keinerlei Auswirkungen für Sie oder das Geld, das Sie am Ende der Studie erhalten! Aber es ist für uns sehr wichtig, dass Sie ehrlich antworten. Kannten Sie bereits vor Teilnahme der Studie Details dazu, was in der Studie passiert? (Type: MC)
Answer Choices: *"Ja", "Nein"*

Q18: Please note that it is important that the questions asked in this questionnaire are answered by each participant independently and without prior knowledge of the study. This ensures the integrity and quality of our data. We therefore ask you not to share any information about the content of the study or the questions of this questionnaire with other people for 2 weeks and your answer to the next question will have no effect on you, your bonus points or bonus payment! But it is very important for us that you answer honestly. Did you already know the details of what happens in the study before participating in the study? *Study2:*Please note that it is important that the questions asked in this questionnaire are answered by each participant independently and without prior knowledge of the study. This ensures the integrity and quality of our data. We therefore ask you not to share any information about the content of the study or the questions in this questionnaire with other people for one week. Your answer to the next question will not affect you or the money you receive at the end of the study! But it is very important to us that you answer honestly.

Before participating in the study, did you already know details about what will happen in the study? (Type: MC)
Answer Choices: *"Yes", "No"*

Q19: Was wusstest du und wie glaubst du hat sich das auf dich ausgewirkt? (Type: Text Entry)

Q19: What did you know and how do you think it affected you? (Type: Text Entry)

Q20: Vielen Dank für das Ausfüllen vom Fragebogen. Wende dich bitte nun an die Person im Raum.

Q20: Thank you for completing the questionnaire. Now please turn to the person in the room.

Quiz (Including Translation)

Participants had to complete a quiz after reading and before starting the scenario. They could answer questions as often until they had all correct.

Q21: Die folgenden Fragen sollen sicherstellen, dass Sie die Aufgabenstellung aufmerksam gelesen und verstanden haben. Sie können alle zur Verfügung stehenden Dokumente zur Beantwortung der Fragen verwenden.

Q21: The following questions are intended to ensure that you have carefully read and understood the assignment. You can use all available documents to answer the questions.
Antwortoptionen: "Alex", "Hannah", "Friedrich", "Eva"

Q22: Was ist der Name der Person, die Sie spielen sollen?
(Type: MC)

Q22: What is the name of the person you are supposed to play?
(Type: MC) *Answer Choices: "Alex", "Hannah", "Friedrich", "Eva"*

Q23: Was sollen Sie tun, wenn Sie eine sichere Verbindung zu einer/m Journalist/in hergestellt haben?
(Type: MC) *Antwortoptionen: "Dem Journalisten die Daten schicken und versuchen, weitere JournalistInnen zu kontaktieren.", "Den Kontakt abbrechen.", "Hannah Bescheid geben.", "Dem Journalisten die Daten schicken. Danach ist die Aufgabe abgeschlossen."*

Q23: What should you do if you have established a secure connection with a journalist?
(Type: MC) *Answer Choices: "Send the data to the journalist and try to contact other journalists", "Cancel the contact", "Let Hannah know", "Send the data to the journalist. The task is then completed."*

Q24: Was sollen Sie tun, wenn Sie nicht sicherstellen können, dass eine Verbindung zu einer/m Journalist/In sicher ist?
(Type: MC) *Antwortoptionen: "Den Kontakt abbrechen.", "Dem Journalisten die Daten schicken.", "Hannah Bescheid geben."*

Q24: What should you do if you cannot ensure that a connection to a journalist is secure?
(Type: MC) *Answer Choices: "Cancel the contact", "Send the data to the journalist", "Let Hannah know".*

Q25: Unter welchen Bedingungen sollen Sie wem die Daten schicken?
(Type: MC) *Antwortoptionen: "Allen JournalistInnen, auch wenn ich nicht sicher sein kann, dass die Verbindungen sicher sind.", "Jedem Journalisten / jeder Journalistin, mit dem/der es eine sichere Verbindung gibt.", "Hannah."*

Q25: Under what conditions should you send the data to whom?
(Type: MC) *Answer Choices: "All journalists, even if I can't be sure that the connections are secure", "Every journalist with whom there is a secure connection", "Hannah".*

Q26: In welchen Situationen erhöht sich die Bonuszahlung? (Mehrfachnennung ist möglich.)
Antwortoptionen: "Eine Verbindung ist nicht sicher und ich schicke keine Daten.", "Eine Verbindung ist sicher und ich schicke Daten.", "Eine Verbindung ist nicht sicher und ich schicke Daten.", "Eine Verbindung ist sicher und ich schicke keine Daten."

Q26: In which situations does the bonus payment increase? (Multiple answers are possible.)
Answer Choices: "A connection is not secure and I am not sending data", "A connection is secure and I am sending data", "A connection is not secure and I am sending data", "A connection is secure and I am not sending data".

Q27: Welche möglichen Situationen kann es in der Studie geben? (Multiple answers are possible.)
Antwortoptionen: "Alle Verbindungen sind sicher und ich schicke allen JournalistInnen die Daten.", "Keine Verbindung ist sicher und ich schicke niemandem die Daten.", "Einige Verbindungen sind sicher und ich schicke dort die Daten."

Q27: What possible situations can occur in the study? (Multiple answers are possible.)
(Type: MC) *Answer Choices: "All connections are secure and I send the data to all journalists", "No connection is secure and I don't send the data to anyone", "Some connections are secure and I send the data there".*

Q28: Welche Aussage stimmt?
(Type: MC) *Antwortoptionen: "Die Angaben auf den Visitenkarten stimmen.", "Die Angaben auf den Visitenkarten können falsch sein."*

Q28: Which statement is true?
(Type: MC) *Answer Choices: "The information on the business cards is correct", "The information on the business cards may be incorrect".*

Interview Guideline

1. Why did you decide to act the way you did with the journalists? (Go through it step by step, was impersonation a conceivable option?)
2. How do you think the methods work? (safety number, QR code, social authentication)
3. Do you have an idea where you would like to apply such a method?
4. Which method would you use if you had to verify a friend? (Focus on why)
5. Would you be willing to use your accounts for social authentication?
6. Would you behave differently as a whistleblower outside of the study?

Businesscards

These are the translated information of the business cards participants had available. All the information except the phone numbers were made up.

Amira

- Amira Patel
- Investigative journalist
- Hallentorstraße 4, 20654 Hamburg
- Phone: {removed as the numbers actually exist}
- Mail: amira_patel@newsorg.de
- Signal Safety Number: 72500 10336 57813 26686 75084 04894

Anne

- Anne Baler
- Investigative journalist
- Isarwege 15, 80542
- Phone: {removed as the numbers actually exist}
- Mail: anne_baler@newsunion.de
- Twitter.com: @AnneBaler
- Facebook.com: Anne_Baler

- *(only Study 1)* Instagram.com: @AnneBaler
- *(only Study 1)* LinkedIn: anne-baler-98746524b
- *(only Study 2)* Amnesty.org: anne-baler-98746524b

Michael

- Michael Kobel
- Investigative journalist
- Maurerweg 28, 10235 Berlin
- Phone: {removed as the numbers actually exist}
- Mail: michael_kobel@newsbody.de
- {Image of a QR Code}

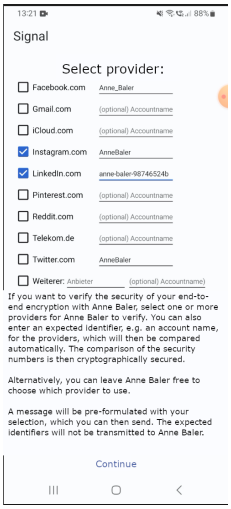
Playbook

This is the playbook the researcher, acting as the journalists, used. It was extended when necessary, and the wording varied slightly from case to case.

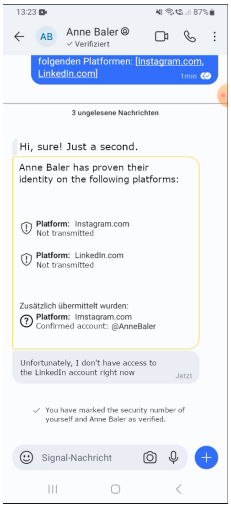
Participant: Hello
Journalist: Hello | Hi | Good morning | Good afternoon | Good evening | Good night
-
Participant: Hello, my name is Alex
Journalist: Hi, I'm [Person Name]
-
Participant: Hi, do you still know me?
Journalist: No, I don't know whose number this is.
Participant: I got your business card some time ago.
Journalist: I give these to a lot of persons. Sorry that I cannot recall you.
Participant: It's me, Alex.
Journalist: Ah, I can briefly remember.
-
Participant: I cannot verify your safety number on the business card. Do you have another idea?
Journalist: Yes, my new number is [safety number].
-
Participant: Can you verify yourself?
Journalist: Yes, I can send you my current safety number.
-
Participant: Your safety number is wrong
Journalist: My number has changed. My new one is [safety number of conversation].
-
Participant: Your QR Code does not match.
Journalist: I lost my old phone and had to buy a new one.
-
Participant: Do you have a [safety number | QR Code] for me?

Journalist: [Current safety number | QR Code sent]
-
Participant: I cannot contact you because Signal says, there is a chance that the conversation is not secure
Journalist: I don't see this message.
-
Participant: Screenshot of failed SOAP message
Journalist: My accounts were hacked before and I had to create new accounts. I don't have new ones on [missing Providers here]. On [changed Username providers], I have a new user handle.
-
Participant: How does your [email, address, phone number, other PII] look like?
Journalist: [Publicly available data]
-
Participant: I would like to send you the data
Journalist: Okay, I'm ready
-
Participant: [data sent]
Journalist: Thank you! I will check the files with my colleagues and get back to you.
-
Participant: [SOAP request]
Journalist: [SOAP response]
-
Participant: Did you arrive safely home?
Journalist: Sorry, do we know each other?
-
Participant: Have you developed any ideas for our project?
Journalist: What do you mean?

D.2 Additional Tables and Figures

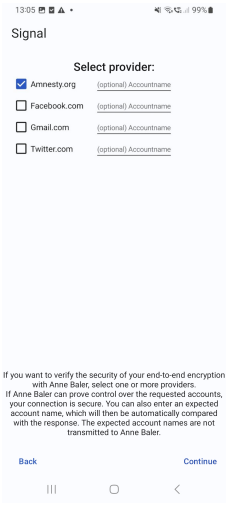


(A) The participant requested two proofs from two providers and filled in the identities.

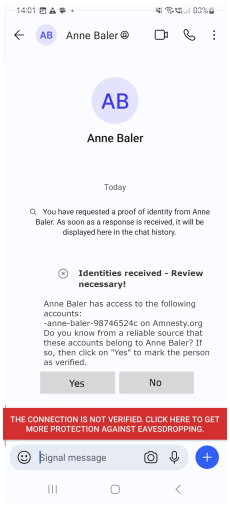


(B) The response was incorrect due to a typo in one identity provider (IdP) and another identifier not being transmitted; however, the participant did not notice the typo and incorrectly marked Anne as verified.

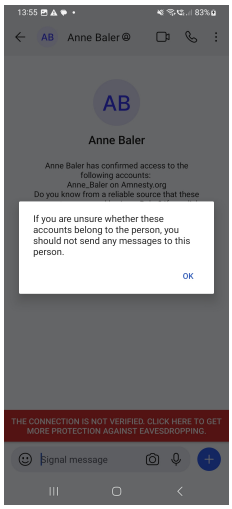
FIGURE D.1: Translated screenshots of the SOAP request flow from P10 (Study 1).



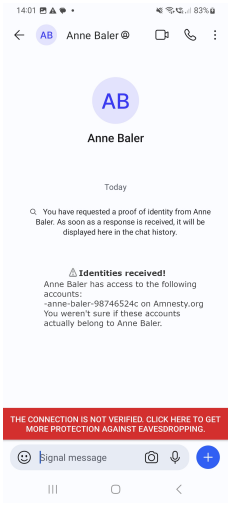
(A) A user can request proof for an account on an IdP without any identity.



(B) As it cannot be automatically decided whether the identifier is correct, the user must make a decision.

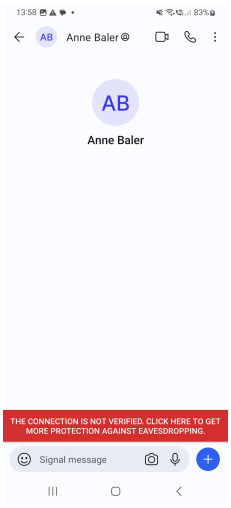


(C) In combination with the decision, the user is informed about possible consequences.

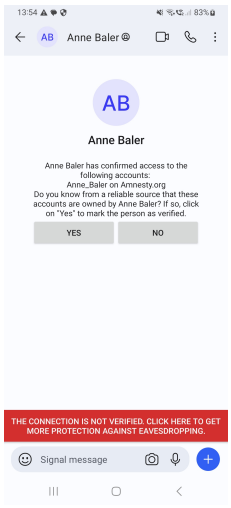


(D) And later reminded what they decided.

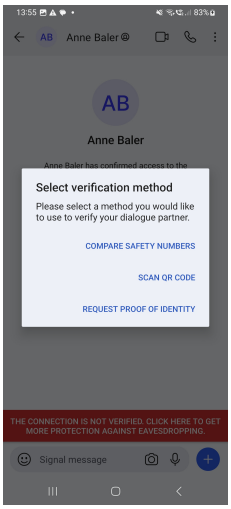
FIGURE D.2: Translated screenshots of a SOAP (study 2 version) request flow without identifiers.



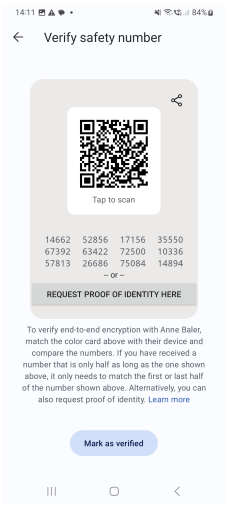
(a) The screenshot shows what a fresh chat looks like if the person was previously added as a contact. The red button nudged the participant to click on it and find the ceremonies.



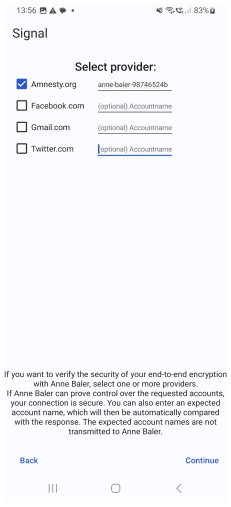
(b) If the participant was in the pre-registration condition, they saw a non-requested SOAP answer.



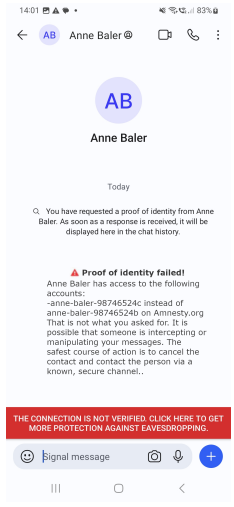
(c) The screenshot shows the menu that led to the ceremonies. Clicking on the QR code and safety number opened the existing site, just slightly modified (see.D.3d).



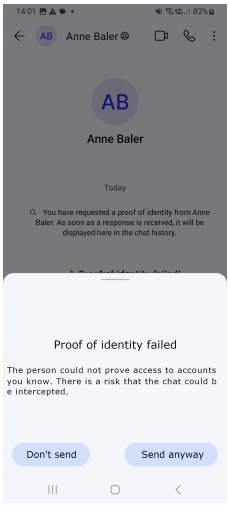
(d) The screenshot shows the menu page where the user can see the safety number, the QR code, and request SOAP. The information text was slightly adapted so that users knew which part of the safety number to compare, and the prompt for social authentication was added.



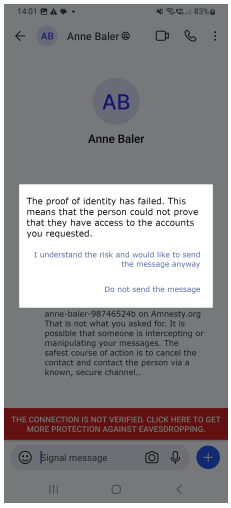
(e) The screenshot shows how a SOAP request code could be made. Selecting an IdP and an identifier. By clicking on next, a SOAP request is sent. The expected identifier is not sent to the recipient.



(f) The SOAP request is sent automatically, and the user is informed in the chat. When the user receives a SOAP response, it is parsed, and compared against the expected identifiers and IdPs. This SOAP response is incorrect, as the identifier is not as expected. The user is informed of that.



(g) If a user wants to send a message to a contact where a SOAP response was incorrect, the app warns the user, similar to when the safety number of a verified contact changes.



(h) To send a message, the user has to click two additional times.

Figure D.3: Translated screenshots of an example SOAP (study 2 version) request flow with expected identifiers filled in.