“You have been in Close Contact with a Person Infected with COVID-19 and you may have been Infected”: Understanding Privacy Concerns, Trust and Adoption in Mobile COVID-19 Tracing Across Four Countries

OKSANA KULYK, The IT University of Copenhagen, Denmark
LAUREN BRITTON-STEELE, Ithaca College, USA
ELDA PAJA, The IT University of Copenhagen, Denmark
MELANIE DUCKERT, The IT University of Copenhagen, Denmark
LOUISE BARKHUUS, The IT University of Copenhagen, Denmark

Through the past two and a half years, COVID-19 has swept through the world and new technologies for mitigating spread, such as exposure notification applications and contact tracing, have been implemented in many countries. However, the uptake has differed from country to country and it has not been clear if culture, death rates or information dissemination have been a factor in their adoption rate. However, these apps introduce issues of trust and privacy protection, which can create challenges in terms of adoptions and daily use. In this paper we present the results from a cross-country survey study of potential barriers to adoption of in particular COVID-19 contact tracing apps. We found that people's existing privacy concerns are an have a reverse correlation with adoption behavior but that the geographical location, as well as other demographics, such as age and gender, do not have significant effect on either adoption of the app or privacy concerns. Instead, a better understanding of what data is collected through the apps lead to a higher level of adoption. We provide suggestions for how to approach the development and deployment of contact tracing apps and more broadly health tracking apps.

CCS Concepts: • **Human-centered computing → Empirical studies in ubiquitous and mobile computing**; • **Security and privacy → Social aspects of security and privacy**.

Additional Key Words and Phrases: e-Health, privacy, trust, health tracking applications

ACM Reference Format:
Oksana Kulyk, Lauren Britton-Steele, Elda Paja, Melanie Duckert, and Louise Barkhuus. 2022. “You have been in Close Contact with a Person Infected with COVID-19 and you may have been Infected”: Understanding Privacy Concerns, Trust and Adoption in Mobile COVID-19 Tracing Across Four Countries. *Proc. ACM Hum.-Comput. Interact.* 6, MHCI, Article 204 (September 2022), 27 pages. https://doi.org/10.1145/3546739

Authors' addresses: Oksana Kulyk, okku@itu.dk, The IT University of Copenhagen, Rued Langgaardsvej 7, Copenhagen, Denmark, 2300; Lauren Britton-Steele, lbritton@ithaca.edu, Ithaca College, Roy H. Park School of Communication, Ithaca, NY, USA; Elda Paja, elpa@itu.dk, The IT University of Copenhagen, Rued Langgaardsvej 7, Copenhagen, Denmark, 2300; Melanie Duckert, mela@itu.dk, The IT University of Copenhagen, Rued Langgaardsvej 7, Copenhagen, Denmark, 2300; Louise Barkhuus, barkhuus@itu.dk, The IT University of Copenhagen, Rued Langgaardsvej 7, Copenhagen, Denmark, 2300.

2573-0142/2022/9-ART204 $15.00
https://doi.org/10.1145/3546739

1 INTRODUCTION

With the global COVID-19 pandemic, contact tracing and exposure notification applications have emerged as an attempted measure to limit spread of the virus, and many countries have developed and released one or more such applications. While some countries successfully developed and distributed national COVID-19 tracing applications, populations in other countries were hesitantly to adopt these types of applications, which were sometimes privately developed. The development of these tools is not new to the COVID-19 pandemic; in the past, tools for tracing Ebola and Zika have significantly strengthened contact tracing and consequently limited disease spread [10]. The general idea behind such apps is to inform people if they have been in close contact with someone who later found out they were positive, in order to quickly isolate and get tested themselves. The increase of individuals with access to smartphones with proximity network technologies, such as Bluetooth, makes the use of these applications more feasible as tools of disease mitigation for current and future diseases. However, the successful deployment of contact tracing depends on the number of people using such applications and their willingness to voluntarily share personal health information when diagnosed. From a privacy perspective, such contact tracing and potential localizing of individuals are complex; a perceived potential misuse or a perceived centralization of personal data can prevent people from adopting such apps. In the beginning of the pandemic, countries took different approaches to the development, distribution, and public awareness initiatives of contact tracing applications, leading to a diverse public understanding of data management strategies and available privacy protections. It is therefore important to understand the underlying hesitance as well as reasoning *for* adoption, in order to design and develop appropriate tracing applications. While exposure notification and contact tracing are not the only tools for limiting disease spread in a pandemic, these applications could function as one of the “Swiss cheese slices” [36] in a broader set of responses to public health crises. Yet, this will only be possible if people are willing to adopt the use of such tools.

In an effort to better understand public perception and use of these tools, we conducted a survey in four countries: Denmark, Germany, Italy, and the United States. The main objective of our study was to explore how existing privacy concerns affected the adoption of COVID-19 contact tracing applications (which we in this article refer to as C19CT apps) across these countries. We analyzed the data guided by the following research questions, with the aim of understanding both population-specific concerns as well as cross-country differences in privacy concerns and adoption rate:

RQ1. What are the differences in attitudes towards various factors of privacy concerns related to COVID-19 tracing apps between the investigated countries?
RQ2. Which factors influence the adoption of COVID19 tracing apps?
RQ3. Which factors influence the privacy concerns regarding COVID-19 tracing apps and how are these factors affected by demographics?

In order to answer RQ1, we study the descriptive statistics of our collected data. For answering RQ2-3, we conduct statistical analyses via logistic and linear regression models as well as exploratory factor analysis.

One factor to be aware of is that the adoption of contact tracing apps was very different between countries, even within Europe. For example, Italy averaged 17 downloads per 100 people whereas Germany averaged 29 downloads per 100 people. Such differences are interesting to explore in relation to individual and cross-cultural factors. And where Denmark, German and Italy had national, highly recommended C19CT apps, the US had multiple privately or state based applications.

While contact tracing applications can potentially be a valuable tool in the fight against a pandemic, the acceptance and general understanding of such applications and their potential consequences should not be underestimated as factors in the overall success rate of such tools. In our study we found that higher adoption rate is associated with lower general concerns about privacy but also associated with a higher level of knowledge of the purpose of the app; we also found that the higher level of trust in organizational entities (such as the government) led to a higher level of adoption.

We conclude by providing suggestions for how to approach the deployment and management of contact tracing apps.

2 PREVIOUS WORK

Due to the COVID-19 tracing applications being fairly new, only a limited set of studies have investigated their implementation and to the best of our knowledge no long-term studies exist yet. We organize the related work according to same themes as the research questions: first we review literature in relation to COVID-19 contact tracing apps, and specifically those that report on (i) influencing factors on adoption of C19CT apps and (ii) user perception of privacy in C19CT apps. Finally, we review past research relating to more general personal data sharing in mobile context, both in regards to location tracking and health data sharing, relating to relevant issues around privacy perceptions. The more specific applications available and referred to in this paper are described further down, in Section 3).

Note that different terminology has been used in both research and public discussions around COVID-19 contact tracing apps, with these types of applications increasingly referred to as "exposure notification applications" (in English), but at the time of the study, and in the most of the countries included in the study, "COVID-19 tracking" or "contact tracing" was the standard term. As mentioned in Section 1, in this paper we refer to these apps as COVID-19 contact tracing apps and shorten them to "C19CT apps", also when referring to studies that used a different term.

2.1 User Adoption of COVID-19 Contact Tracing Apps

Since several countries started developing digital contact tracing apps to support their manual[1] tracing of COVID-19, researchers around the world have attempted to understand users' willingness to adopt these apps.

Studies have in particular been conducted in European countries (e.g., Germany [6, 13, 17, 30, 52], Switzerland [50], France, [37]), the United States [25, 26, 28, 42] and Australia [47], where several of these have been conducted as cross-country studies comparing different populations' app adoption [1, 12, 22, 48]. These studies found that the actual adoption rates for most C19CT apps, are lower than what is needed for the apps to have a significant effect on mitigating the pandemic [6, 22, 24, 28, 32, 52].

A number of possible reasons behind the low adoption rates have been explored, related to such aspects of C19CT apps as the app characteristics including available functionality and user experience [22, 31, 32], personal circumstances of the the user [28], such as whether they knew someone who died from COVID-19, their health concerns, privacy concerns and trust in the government [1, 17, 23, 30], perceived usefulness of such apps [42] and a more complex combination of factors [6, 32].

Our study complements existing work, emphasizing the importance of several factors identified in related work – privacy concerns and trust in the government – as well as further factors such as trust in other involved entities such as software development companies involved in the creation and distribution of C19CT apps and understanding of how the app works across four countries.

[1] Manual tracing often includes calling up a newly infected person, asking them to provide contact information of all the people they have been in contact with the previous 48 ours or more.

2.2 User Perception of Privacy

As described above, several studies found privacy to be a widespread concern and this can be a considerable factor influencing app adoption [1, 22, 31, 32, 43, 48, 52]. More explicitly research found that people worry about C19CT apps to be "surveillance tools" [31, 48, 52], which could make them reluctant to download the app [37, 52]. In particularly participants from German-speaking countries [52] perceived C19CT apps as "governmental surveillance tools", however having different perceptions of whether this surveillance is justified due to the pandemic. Correspondingly, several measures were proposed as ways to alleviate privacy concerns, such as referring to C19CT apps as "exposure notification apps" and overall transparent communication of what data the app collects[1, 30, 31, 48]. Other studies however, did not find privacy concerns to be among the main influencing factors when deciding to install an app [6]. Comparing privacy attitudes of participants from different countries, Altman et al. found that respondents from Germany and the United States were be more likely to mention concerns about privacy, security, and governmental surveillance, compared to participants from France, Italy and UK [1].

Other studies have focused on perceptions of more detailed technical workings of the specific apps – in particular, regarding their data collection and sharing policies. Häring et al. studied the German populations' knowledge immediately before the release and found that many participant were missing information or had beliefs about the app that were not true [17], such as believing that the app collected location data, which is not true as it uses Bluetooth to proximity detection [17]. Two other studies [25, 51] investigated the US users' perception and preference of two data collection models: the *decentralized* model, where most of the data is stored on users' device, and *centralized*, with authorities having much more extensive access to the users' personal data. The findings were conflicting: Li et al. found people to prefer to install C19CT apps that is centralized [25] while Zhang et al. found people to be more acceptable of a C19CT apps with a decentralized architecture [51].

Similar to most of these studies, we identify privacy concerns to be an important factor in deciding to adopt the app. Our study confirms the need of transparent communication, showing that lack of knowledge about the app and corresponding belief that the app is more privacy-invasive than it is designed to be, is a factor than can negatively influence adoption. We furthermore find that the participants in our survey across different countries were less concerned over using the C19CT app with a decentralized model.

2.3 Sharing of Location Data

Since all literature related explicitly to C19CT apps is fairly new, we also briefly review privacy studies concerning sharing location and health data more generally, particularly due to people's common perception that C19CT apps use their personal location data. Location sharing apps are not new in any sense, and early research looked for example at people's willingness to share location data (e.g., [4, 8, 9, 29]). Personal location sharing is almost exclusively facilitated through smartphones, for example through GPS-based map pointers or descriptive tags in social networks such as Facebook check-in [41]. Motivations to share location can be diverse and relevant for different contexts, from social grooming to parents' surveillance of teenage children [27, 46].

Previous studies found that people can be positive towards location-based services as long as they perceive them to be useful [4]. Within social relations, people would be willing to share the location data that was *useful* for the receiver independent of how precise the location was; they would either give the most useful information, including the precise position, or not give any data at all [9]. This resonates with a potential perceived usefulness of sharing COVID-19 infection status to protect people's health. Brush et al. found people to prefer different location obfuscations strategies, and that privacy control interfaces should provide users with informed choices [8].

In a health context, Murphy et al. found young adults to be positive about sharing mobile phone location data to improve public healthcare [29]. Moreover, they argued that more education on data collection, storage and protection can "ease concerns and prevent hesitancy" toward location data sharing [29].

3 BACKGROUND: COVID-19 CONTACT TRACING APPS

In this section, we describe the current C19CT apps in the four different countries where we conducted the survey. Their development were for obvious reasons mostly rushed, and in some countries, one approach was started, only to be abandoned months into development and another approach adopted. One major difference between the four countries is that where the EU countries developed national government affiliated (and sometimes government sponsored) applications, the US provides private and state based applications, but does not have one nationwide recommended app. Another important thing to keep in mind is that one phone can only have one active C19CT app at any given time. This also means that for travel, a user has to manually download the new country's app, pause the old one and activate the new one.

In the US the first wave of C19CT apps was launched in August 2020 but covers today nearly half (24) of the US states (with 32 apps in total, some covering more than one state) [39]. The majority of the apps rely on the API developed by Apple and Google, which uses Bluetooth to trace people who have been near you and later diagnosed with COVID-19, however different developers can make use of and customize different parameters of their API which is why the C19CT apps will be different in different states/countries. For example, the version developed in Alabama works with exposure notifications apps from other states, in Michigan and Virginia a list of anonymous data may be shared with other entities for statistical and research purpose, in North Dakota the tracing app is used in additional to a diary app, and in Wyoming data are send to a third party to improve app performance [39]. Among the states that do not make use of Apple and Google's API, four use location data. This is for example the case in South Dakota where their Department of Health will reach out to a person if they test positive for COVID-19, ask them if they use the app and request them to share their locations [39].

The Danish national app "Smittestop" was provided by the governmental authorities and a Danish publicly traded IT company. It builds on Apple and Google's API and as such uses the smartphone's Bluetooth to trace other people's smartphones. To ensure anonymity, the ID is updated within 20 minutes with a rolling system-generated ID. The Danish C19CT app was launched June 18, 2020, and is voluntary to download just as it is voluntary to register if you have a positive COVID-19 test result. A user has to register a positive test results themselves, although this registration is checked by the health authorities to ensure only valid test results are registered. Users will only receive a notification of contact to a COVID-19 positive if the encounter lasted for more than 15 minutes (based on the duration) and the distance was less than one meter (based on the strength of the Bluetooth connection) [44]. A few months after the launch, the app was criticized for not always providing notifications of exposure, which was argued to be due to the developers focusing on 'random meetings', e.g. in the bus, why users would not always get notifications at longer meetings such as other household members and colleagues [14]. At the end of 2020, the app was again criticized for missing notifications, this time on Android phones, where users had to check the app for encounters with exposure as the notification system did not always work [45]. At the time the study took place, winter 2020/2021, the app had around 2.1 million downloads, which corresponds to around 36% of the population.

The Italian app was tested in four regions before the government extended it to the whole country in June 2020. It builds on Apple and Google's API and was developed by a Milan based tech start-up [2]. If a person is tested positive for COVID-19, the doctor has to upload the result anonymously in the health system, get a code that has to be uploaded to the C19CT app and send this code to the patient who also has to upload it to the C19CT app; the process was criticized for being vulnerable as several actions from different people are needed and sometimes either the doctor or the patient would not do it correctly [21]. If a user has been a close contact to a COVID-19 positive, they will get a notification telling them to self-isolate and get tested [34]. In October 2020 it was discovered that the app did not work on all iPhones and users would not always receive notifications on exposure but had to open the app to see encounters with COVID-19 positive users [5]; the same problem that was experienced with the Danish app. At the time of the study, the Italian app had 9.9 million downloads [38], which represents approximately 16% of the population.

The German app "Corona-Warnapp" [35] was released to the general public in June 2020. Similar to other apps used in European countries, the app built on the decentralised solution implemented by the Apple and Google's API, using Bluetooth information to track close contacts with infected people without revealing the identities of the users. It was developed in cooperation of public and private institutions: the German Robert-Koch Institute and the companies Deutsche Telekom and SAP. Downloading the app, as well as entering one's positive COVID-19 result, is voluntary but encouraged. As an effort to introduce transparency into the app, the source code was published on Github prior to the app release [15]. In addition to exposure notification functionality, the app introduced additional features, such as a "contact journal" allowing the users to keep track of people they met [18]. While using these additional features would potentially have the user share more data with the app in addition to the Bluetooth tokens, the app developers stressed that these features are voluntary and work decoupled from the main contact tracing system [19]. Similar to the Danish and Italian app, the users of the app experienced technical issues, such as the app stopping to work after a software update on one's phone [16]. At the time of the study, the app had 23.2 million downloads [20] (approximately 28% of the German population).

4 METHOD

In an aim to understand specific privacy concerns in relation to adoption rate and use of specifically C19CT apps, we conducted a cross-country survey inquiring into a wide set of uses, the understanding of the relevant information tracing apps and data sharing concerns. We chose to include four countries, three within Europe: Denmark, Germany and Italy, as well as the US, with a presumption that the results from US residents would likely look different from that of the European residents. We specifically chose Denmark, Germany and Italy for two main reasons: (i) their perceived difference in culture (Northern European, Central European and Southern European), and (ii) the convenience of the authors being proficient in all three languages, enabling original language analysis and a deep understanding of the phrasing of the questions. The authors were also all deeply involved in the culture of these countries, which led to a greater understanding of the context of the country during the COVID-19 crisis. While we relied on a small level of external translation and checking of the naturalness of questions, being fluent in all languages (as well as of course English), proved very useful for our team in the analysis phase.

4.1 Development of the Survey

The survey was initially developed as a questionnaire in English; all researchers went through the questions multiple times, and several smaller pilot tests were conducted. Secondly, the survey was translated into the three other languages: Danish, German and Italian, and for each one of the translations, a native speaker who was not involved in the original development of the questionnaire provided their feedback. Pilot tests of the questionnaires in each of these languages were conducted too [2]. Participants were given the option to answer it in any of these provided languages. That meant that a small subset of all the European participants answered it in English, either because they did not know the local language of the country from which they completed the questionnaire, or because they felt more comfortable in English. While we could not check for legal residency, the survey was checked for location at the time of it being answered.

Survey design. At the beginning of the survey, the participants were given the option to choose the language (Danish, English, German or Italian), followed by a welcome message introducing the purpose of the study, its benefits, and what the participant would be asked about, followed by the consent form. The survey consisted of a total of 31 questions, divided across 9 sections. As our goal was to study the different demographic and privacy-related factors affecting the adoption and perceptions of local C19CT apps, the questions aimed to focus on different aspects of data collection and usage of these apps, asking about either the participants' behavior or their attitudes regarding these aspects. The first section was asking questions to position participants in terms of their confidence with technology and awareness of and experience with C19CT apps, while the last section posed questions to capture participants' demographics. The remaining sections posed questions related to participants' concerns on potential privacy issues, their understanding of the data collection models (the presented models were based on the workings of commonly available apps as well as media discussions around the concept of such apps), the purpose of using C19CT apps, their trust in various entities (the government, private/public organizations), their beliefs with respect to data collection/storage/usage, their willingness to share location information at different levels of granularity and/or with different stakeholders.

The estimated time to complete the survey was 10 minutes. We have included the survey questionnaire with the supplementary materials for the paper.

4.2 Deployment of the Survey

The survey was distributed through crowdsourcing market place platforms in all countries except Denmark where this was not a possible data collection method (no national crowdsourcing tool exists and when aiming to get Danish residents through other tools, no answers were provided).

Table 1. Participant Demographics

	Denmark	Germany	Italy	United States
Average Age	36.8	29.8	31.2	45.5
Female/Male/Non-binary	53/53/0	73/63/1	64/79/1	74/51/0
Share of participants with university-level education	62.0%	65.2%	53.5%	64.8%
Average self assessed technical proficiency (1–5)	4.39	4.46	4.42	4.17

In Germany and Italy the platform Prolific[3] was used and in the US Amazon's Mechanical Turk[4] was used. In the US participants were paid the recommended average of USD 1.5 per survey and in Germany and Italy they were paid the recommended average of EUR 1.5 per survey. We supplemented both the Italian and the German data collection with social media postings, in order to broaden the sample to a higher age group and with a higher level of education, since Prolific seemed

[2] Note that these translations were not trivial; as well as translating words and terminology directly, we also went through phrasings with native speakers not affiliated the project, to make sure that the questions made sense and sounded natural in the language in question. Occasionally we had to compromise a direct translation with local terminology: for example in German the more commonly used notion of "go into self-quarantine" ("sich in Selbstquarantäne begeben") was used instead of "self-isolate".

[3] https://prolific.co, last visited September 9th, 2021

[4] https://www.mturk.com, last visited September 9th, 2021

Table 2. Share of US participants selecting each option for race. Note, it was possible to select multiple options.

White or Caucasian	76.8%
Black or African American	10.4%
Asian or Pacific Islander	7.2%
Hispanic or Latinx	5.6%
Multiracial or Biracial	1.6%
Native American or Alaskan Native	0.8%
Other	1.6%

to cater to a younger group, particularly compared to Mechanical Turk in the US. In Denmark we used purposeful sampling, posting on social media, sending direct requests to mailing lists, in an aim to get a wide set of respondents. While it does not provide a set of 'average' Danish residents, the data set is close enough in demographics that is comparable to the other samples. We checked for age, gender[5], education level, but also technology proficiency; Table 1 shows the averages and ranges for all four countries. As it may be noted Germany stands out slightly with a lower average age, and this was taken into account during the analysis. For the US participants we also asked for race/ethnicity, see Table 2, however for the European participants, the question was deemed inappropriate in the pilot test.

The survey was conducted between December 2020 and end of February 2021, at the height of the second larger wave of COVID-19.

4.3 Ethics

While the main research institution involved does not have a mandatory Institutional Review Board (IRB) for studies, for the secondary research institution involved, we got IRB approval. Nevertheless, the main research institution addressed the four considerations related to ethics in conducting such a research: informed consent, confidentiality, consequences and the role of the researcher [7, 11]. Specifically, we protected the confidentiality of the participants, assuring them that their personal data will not be shared with anyone and that the results will only be reported in anonymized form. Most importantly, even though the survey is on health tracking applications, no participant was asked to provide health data. We explicitly informed our participants about the purpose of the survey, and informed them of their right to withdraw from (aka interrupt) the survey at anytime. Finally, we did not provide any remuneration to participants recruited through snowballing and/or via leveraging our personal and professional networks, while as stated earlier we paid participants that were recruited through the Prolific platform and Amazon Mechanical Turk.

4.4 Limitations

While the survey was distributed in a concentrated time frame in Germany, Italy and the US, the survey was distributed over the full timeframe in Denmark, due to the lack of a data collection instrument. We also had to supplement the other initial datasets with snowball sampling to increase participation and to get closer to a similar average age for the samples. Our survey focused on privacy attitudes, which might have primed the participants in thinking more about privacy-related issues. Hence, it is possible that some of our participants expressed higher privacy concerns than they had in their daily life, when they are not confronted with data protection issues related to

[5] Two participants preferred not to report their gender.

C19CT apps. However, since these issues have been frequently touched upon in public discussions around C19CT apps, we consider the additional priming effects to be acceptable.

5 RESULTS

We collected a total of 512 responses, where 108 were from Denmark, 135 from Germany, 144 from Italy and 125 from the US. Additionally, we performed a quality check on the survey responses by removing incomplete entries and reviewing all open-ended questions for possible spam-like entries. Before the final number of 512, we had removed 90 responses for being incomplete and found no instances of spam-like entries in the data. For the analysis of RQ2 (i.e. factors influencing adoption of the app) we removed the participants who reported not owning a smartphone or not knowing about any of the C19CT apps they could install, as these participants could not be expected to install the app regardless of the other factors. This resulted in the removal of 11, 11, 9, 74 answers from Denmark, Germany, Italy, US respectively. For the two other RQs we used the full datasets.

We first report our general findings based on descriptive statistics answering our main research question: *what are the differences attitudes towards various factors of privacy concerns related to C19CT apps between the investigated countries?* (RQ1). We follow by looking deeper into the other research questions that we evaluate via statistical analysis: *which factors influence the adoption of C19CT apps* (RQ2), *which factors influence the privacy conncerns regarding the C19CT apps* (RQ3) and *how are these factors affected by demographics*.

We used R packages “stats”, “ordinal”, “emmeans” and “psych” for the analysis. In order to reduce the dimensionality of the data, we aggregated the responses on items that were grouped together in the questionnaire (e.g. participants expressing their trust in various entities developing the app, which we will expand on in the subsections below.

.

5.1 Differences in Attitudes Towards C19CT apps Between the Countries (RQ1)

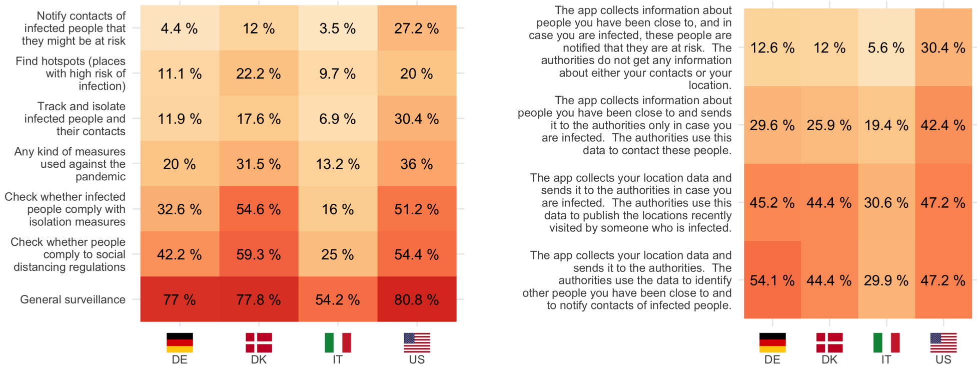
Looking at descriptive statistics for specific questions, the following patterns emerged regarding the differences between the countries.

5.1.1 Attitudes towards data sharing and usage by the app. A number of questions focused on participants’ attitudes towards C19CT apps in general, such as their willingness to share particular data with the app or use the app for specific purposes.

Purposes of using the app. Very few participants from all of the countries were unwilling to use the app for purposes directly related to tracking the spread of the pandemic, such as notifying contacts of infected people (between 3.5% unwilling in Italy to 27.2% unwilling in the US), finding hotspots of infection (from 9.7% unwilling in Italy to 20% unwilling in the US), tracking infected people and their contacts (from 6.9% unwilling in Italy to 30.4% unwilling in the US) and other kinds of measures against the pandemic (from 13.2% unwilling in Italy to 36% unwilling in the US), see Figure 1a. However, the majority of participants in each country were unwilling to use the app for the purpose of general surveillance (from 54.2% in Italy to 80.8% in the US).

In comparing responses by country, we find that participants from Italy were most willing to share their data, while participants in the US were least willing. Of the European countries, participants from Denmark were least willing to use the apps for purposes related to compliance enforcing, like checking whether people were complying with social distancing measures (54.6% unwilling) and with self-isolation requirements (59.3% unwilling).

Attitudes towards data collection models. All participants across the countries were more comfortable with a decentralized data collection model – i.e. the model where the authorities get limited or no access to the data collected by the app, see Figure 1b. Still, participants from the US were less comfortable with this model models compared to participants from Europe (12.6%, 12%, 5.6%, 30.4% uncomfortable in Germany, Denmark, Italy, US), and participants from Italy were most comfortable with all the presented data collection models, including centralized ones (with 29.9% in Italy being uncomfortable with the model that involves the most invasive data collection, as opposed to 54.1%, 44.4%, 47.2% being uncomfortable with such a model in Germany, Denmark, US).

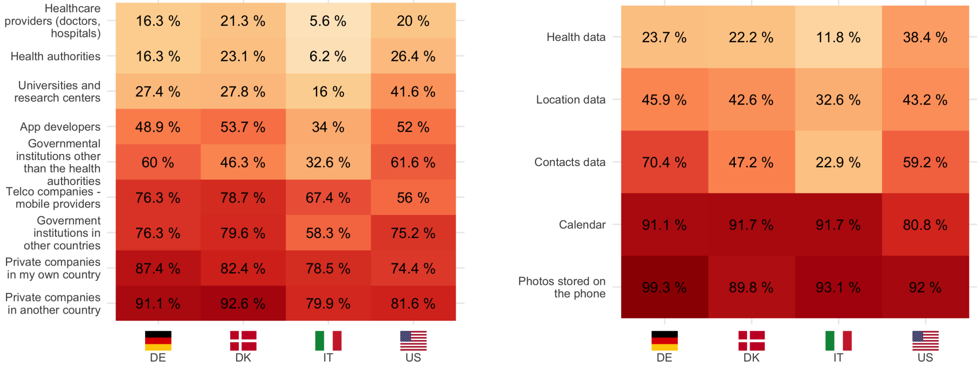


(a) Unwillingness to download the app if it is used for a particular purpose (showing percentage of participants either "somewhat not willing" or "not willing" to download the app)

(b) Being uncomfortable with particular data collection models (showing percentage of participants either "somewhat not comfortable" or "not comfortable" with a particular model)

Fig. 1. Attitudes towards purposes and data collection models

Attitudes towards sharing data from the app with different entities. Most of the participants in each country were willing to share the data from the app with healthcare providers (from 5.6% unwilling in Italy to 21.3% unwilling in Denmark), health authorities (from 6.2% unwilling in Italy to 26.4% unwilling in the US) and universities and research centers (from 16% unwilling in Italy to 41.6% unwilling in the US), see Figure 2a. However, participants from the US were significantly more negative about providing their data to universities and research centers when compared to the participants from the European countries (27.4%, 27.8%, 16% unwilling to share their data with these entities in Germany, Denmark and Italy). Around half of the participants in Germany (48.9%), Denmark (53.7%) and the US (52%) were not willing to share their data with the app developers, while only a third of participants in Italy (34%) had similar attitudes. Participants from Germany and the US were more negative towards sharing their data with governmental entities other than health authorities (60% in Germany and 61.6% in the US unwilling to share their data, compared to 46.3% in Denmark and 32.6% in Italy). The majority of participants from all the countries were unwilling to share their data with either mobile providers (from 56% in the US to 78.7% in Denmark), governmental institutions in other countries (from 58.3% in Italy to 79.6% in Denmark), and both domestic (from 74.4% in the US to 87.4% in Germany) and foreign (from 79.9% in Italy to 92.6% in Germany) private companies. Consistent with our other findings, participants from Italy were more willing to share their data with governmental institutions than participants in other countries. While participants from the US expressed far more negative attitudes overall, they were more willing to share their data with mobile providers than our European participants.



(a) Unwillingness to share data from the app with different entities (showing percentage of participants either "somewhat not willing" or "not willing" to share their data)

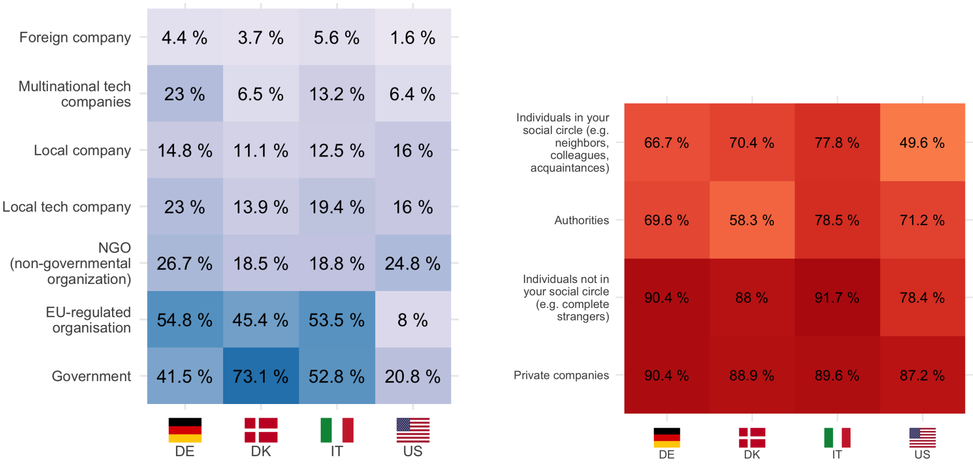
(b) Unwillingness to share different types of data with the app (showing percentage of participants either "somewhat not willing" or "not willing" to share their data)

Fig. 2. Attitudes towards sharing specific data types and specific entities with access to data

Attitudes towards sharing different types of data with the app. Most of the participants from all countries were willing to share their health data with the app, see Figure 2b, although the participants from the US had a more negative attitude (38.4% unwilling to share their data) compared to the participants from Europe (23.7% unwilling in Germany, 22.2% in Denmark and 11.8% in Italy). Participants from Germany had the most negative attitudes towards sharing their contact data with the app, followed by the participants from the US (70.4% unwilling to share, compared to 47.2%, 22.9%, 59.2% in Denmark, Italy and the US); participants from Italy were most willing to share their health data, location data (32.6% unwilling to share, compared to 45.9%, 42.6%, 43.2% unwilling in Germany, Denmark and the US) and contact data. In all of the countries, the overwhelming majority of the participants were unwilling to share their calendar data (from 80.8% in the US to 91.7% in Denmark and Italy) and photos stored on their smartphone (from 89.8% in Denmark to 99.3% in Germany) with the app.

Trust in entities related to the app. The participants had diverse attitudes towards trusting particular entities in developing and maintaining the app, see Figure 3a. While many of participants from European countries trusted EU-regulated organizations (54.8%, 45.4%, 53.5% in Germany, Denmark, Italy), only 8% of the participants from the US had trust in such organizations. Moreover, similar disparities were shown in participants' trust in their own governments; while many of the participants in European countries, most notably in Denmark (73.1%) but also in Germany (41.5%) and Italy (52.8%) trusted their government regarding the app, only 20.8% of the participants from the US expressed such trust. The rest of the entities were trusted only by a minority of the participants, with the least trust put into foreign governments (4.4%, 3.7%, 5.6%, 1.6% in Germany, Denmark, Italy, US).

Concerns about unauthorized access to the data from the app. Participants from all the countries were concerned about unauthorized access by all kinds of entities, especially by private companies (from 87.2% in the US to 90.4% in Germany), see Figure 3b. Still, participants from Denmark were less likely to be concerned about unauthorized access by the government (58.3%, as opposed to 69.6%, 78.5%, 71.2% from Germany, Italy, US), and the participants from the US were less likely to



(a) Percentage of participants trusting a particular entity for developing and maintaining the app

(b) Being concerned about unauthorised access to the data collected by the app (showing percentage of participants either "somewhat concerned" or "very concerned")

Fig. 3. Trust towards specific entities responsible for the app and concerns about unauthorized access

be concerned about unauthorized access by individuals in their social circles (49.6%, as opposed to 66.7%, 70.4%, 77.8% in Germany, Denmark, Italy) as well as outside their social circles (78.4%, as opposed to 90.4%, 88%, 91.7% in Germany, Denmark, Italy).

5.1.2 *Understanding of how the app works.*

Further questions focused on finding out the level of understanding by the participants on how current C19CT apps work, such as what data was collected by the app or which entities had access to this data.

Entities having access to the data from the app. The majority of participants in all countries believed that the government had access to the data collected by the app (from 54.1% in Germany to 73.6% in the US), and around half of participants in all countries believed that the data is accessed by either health care providers (from 40.7% in Germany to 56% in the US) or app developers (from 42.2% in Germany to 64.8% in the US), see Figure 4a. Only a minority of participants in all countries believed that the data was accessed by mobile providers (from 13% in Denmark to 38.4% in US). Overall, the participants from the US were more likely to believe that the data can be accessed by all of the entities mentioned in the survey.

Location of data storage. The participants from the US and from Italy were more likely to believe that the data is stored in some centralized manner (see Figure 4b); as such, 73.8% of US participants believed that it is stored centrally in some company (as opposed to 38.5%, 32.4% and 44.4% of participants in Germany, Denmark and Italy correspondingly), and 56.2% of participants from Italy believed that it is stored centrally with the government (as opposed to 28.9%, 43.5% and 46.4% in Germany, Denmark and US). Participants from Denmark were almost equally likely to believe that the data is stored either locally or centrally with the government (47.2% and 43.5% correspondingly), while the participants from Germany mostly believed that the data is stored locally only, with only 28.9% and 38.5% believing in central storage with either the government and companies.

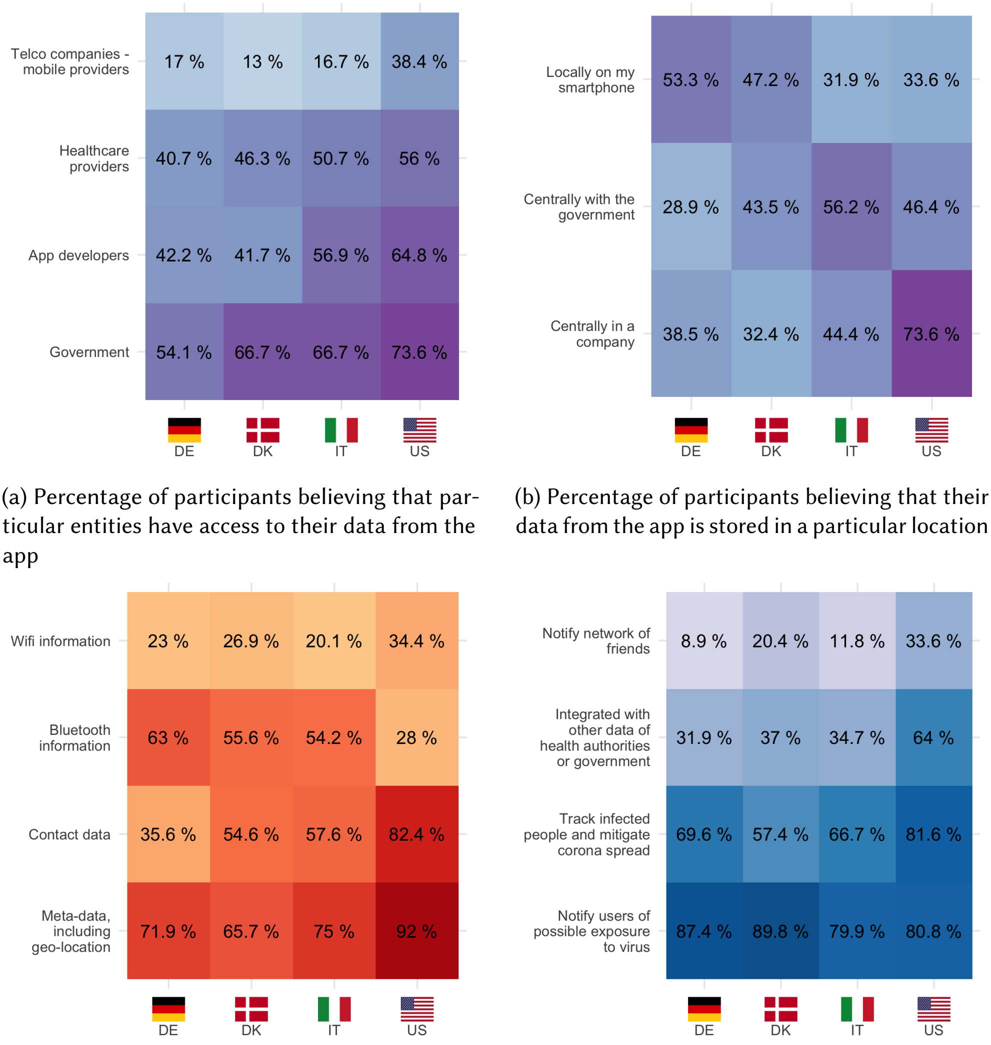
Collection of specific data types. The majority of the participants in all the countries believed that the app collected meta-data including geo-location, with such beliefs being especially overwhelming among the US participants (71.9%, 65.7%, 75%, 92% in Germany, Denmark, Italy, US correspondingly), see Figure 4c. Similarly, the participants from the US were much more likely to believe that the app collects contact data (82.4% in US as opposed to 35.6%, 54.6%, 57.6% in Germany, Denmark, Italy). On the contrary, the participants from Europe were much more likely to believe that the app collects Bluetooth data (63%, 55.6%, 54.2% in Germany, Denmark, Italy; 28% in the US). Only a minority of participants in all countries believed that the app collects WiFi information (from 20.1% in Italy to 34.4% in the US).

Purposes of using the data from the app. The majority of the participants in all countries believed that the data from the app is used for notifying the app users about a possible exposure (from 80.8% in the US to 89.8% in Denmark), as well as for tracking infected people and mitigating the COVID-19 spread (from 57.4% in Denmark to 81.6% in the US), see Figure 4d. The participants from the US were more likely to believe that the data is also used for broader purposes, namely, notifying the network of friends (33.6% in US, compared to 8.9%, 20.4%, 11.8% in Germany, Denmark, Italy) and integration with other kinds of data collected by the government (64% in the US, 31.9%, 37%, 34.7% in Germany, Denmark, Italy).

5.1.3 General attitudes towards data sharing. We also asked the participants about their general willingness to share their location and proximity data with a number of entities. Overall, participants in all countries were most likely to be willing to share their both location and proximity data with family and friends, and least likely to be willing to share this data with private companies and the general public, see Figure 5. Our participants from Denmark, nonetheless, were less likely to be willing to share their both location and proximity data with friends (43.5% unwilling to share location, compared to 25.2%, 36.1%, 23.2% in Germany, Italy, US; 41.7% unwilling to share proximity, compared to 23%, 35.4%, 27.2% in Germany, Italy, US). Participants from Italy and Denmark were furthermore less likely to share their data with family outside of their household (34.7% unwilling to share location in Italy and 29.6% in Denmark, compared to 19.3% in Germany and 16% in the US; 38.2% unwilling to share location in Italy and 30.6% in Denmark, compared to 18.5% in Germany and 19.2% in the US).

5.1.4 Summary. Overall, the US participants in our sample were less informed about the features of state-of-the-art COVID-19 apps, as well as more skeptical of their level of privacy protection. As such, they were more likely to believe that the data is stored in a centralized way, that more types of data are collected and that those data are used for more broad purposes than just mitigating the pandemic. At the same time, the participant from the US were more likely to be concerned about proper protection of collected data, being less trustful towards all types of entities, especially governmental institutions, compared to our participants from the European countries.

Out of the participants from the European countries, the participants from Italy were most willing to use the app for an extensive variety of purposes, as well as share more extensive data with the app. Participants from Germany showed the most skepticism towards potential data collection and usage by the app compared to the European countries, and at the same time being more likely to believe in limited data collection compared to the rest of European countries. Participants from Denmark, while also being skeptical about certain privacy implications of the app (e.g. purposes of use and sharing certain kinds of data), showed the highest levels of trust in their government in developing and maintaining the app.



(a) Percentage of participants believing that particular entities have access to their data from the app

(b) Percentage of participants believing that their data from the app is stored in a particular location

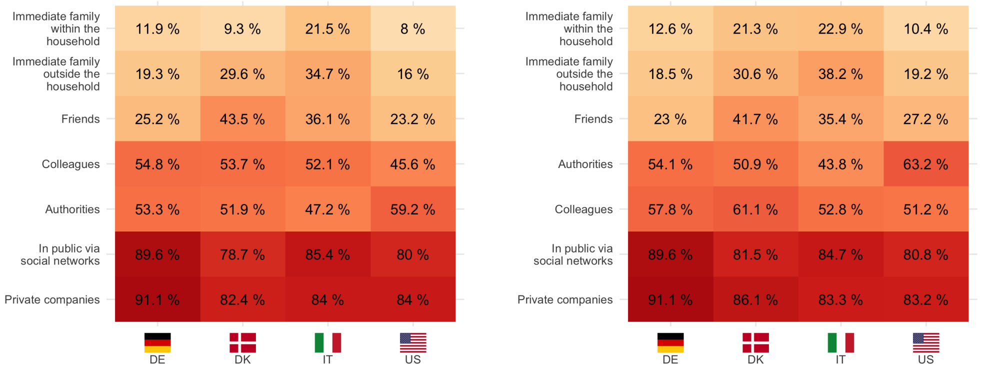
(c) Percentage of participants believing that a particular data type is collected by the app

(d) Percentage of participants believing that the data from the app is used for a particular purpose

Fig. 4. Answers to questions related to the participants' understanding about data collection and usage by the app

5.2 Factors Influencing Adoption of COVID-19 Contact Tracing Apps (RQ2)

Overall 284 participants of our study reported installing a C19CT app, (55.4%), of them 185 (36.1%) reported keeping it turned on at all times. While the European countries had similar and comparably high adoption rates, the US stood out with only 19.2% of participants installing such app (see Figure 6).



(a) Unwillingness to share one's location (showing percentage of participants either "somewhat not willing" or "not willing" to share their location with corresponding parties)

(b) Unwillingness to share one's proximity (showing percentage of participants either "somewhat not willing" or "not willing" to share their proximity information with corresponding parties)

Fig. 5. Answers to questions related to general data sharing

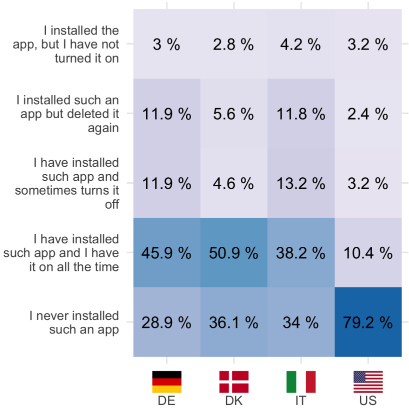


Fig. 6. Percentage of participants checking either variant of (not) using the app

We built a logistical regression model with people's decision to install the C19CT apps as the output[6], looking at following predictors: (1) demographic factors: age, gender, education (grouping into university-level and below university-level education) and experience with technology (aggregating self-reported technology proficiency and whether the participants reported daily use of a computer), (2) privacy concerns (as asked via a direct question within the survey, measured on a scale from 1 = very concerned to 4 = not concerned at all), (3) willingness to trust in different entities developing and maintaining the app (as total number of entities the participants selected as someone they would trust), (4) how comfortable the participants are with use the app for diverse purposes. The resulting model is provided in Table 3 (omitting non-significant predictors with

[6] Note, for the sake of the analysis we did not distinguish between people installing the app and turning it off or deleting it afterwards, investigating the initial decision to install the app instead.

$p > .05$[7]). The factors that reached the level of statistical significance were: having a university-level education (with people with such education being more likely to install the app), experience with technology (with people who are more experienced also being more likely to install the app), awareness about the apps (with participants aware about the official app recommended by the government more likely to install it), privacy concerns (people more concerned with privacy being less likely to install the app), and being comfortable with both covid-related and non-covid-related purposes (see Figure 1a of using the app (the higher the average score of comfort for all the proposed purposes[8], the more likely the participants were to install the app). The post-hoc pairwise tests for the categorical predictors in the model did not reveal any further significant factors.

term	estimate	std.error	statistic	p.value
university	0.65	0.29	2.21	0.0274
technology_aggr	0.43	0.16	2.74	0.0061
awarenessOfficialApp	2.22	0.68	3.26	0.0011
privacy_concerns	-0.71	0.15	-4.64	< 0.0001
purposes	0.09	0.03	2.96	0.0031

Table 3. Logistic regression model (only significant predictors) for RQ1

5.3 Factors Influencing Privacy Concerns Regarding COVID-19 Contact Tracing Apps (RQ3)

We also looked at how concerned people expressed being, in relation to their privacy when potentially using C19CT apps. The majority of our participants (69%) were either “not concerned” or “slightly concerned” about their privacy when using the C19CT apps, with the breakdown into countries showing heightened concerns of the US participants compared to the participants from European countries, see Figure 7.

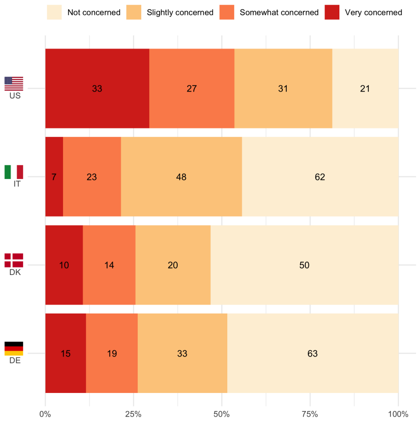


Fig. 7. Privacy concerns of participants related to the usage of C19CT apps (showing number of participants for each level of concern)

[7] For the analysis results for all the predictors, see Appendix B

[8] Cronbach’s alpha for questions about individual purposes is 0.885.

To understand the details of these findings a bit better we conducted a principal component analysis on the following variables related to privacy: (1) average score[9] of being generally comfortable to share one's location with different entities, (2) average score of being generally comfortable to share one's proximity information with different entities, (3) average score of being comfortable in sharing different types of data with the app, (4) average score of being comfortable to share the data collected by the app with diverse entities, (5) number of data types the participant believes the app collects, (6) whether the participant believes that the data is stored only locally, centrally either with the government or a private company, or centrally both with the government and a private company, (7) number of entities[10] the participant believes the data from the app is shared with, (8) number of entities the participant is willing to trust to develop and maintain the app, (9) average score of being concerned with unauthorised access to the app by different entities, (10) average score of being comfortable with diverse models of data collection, (12) average score of being comfortable with using the app for diverse purposes, (11) number of different activities one believes the data from the app is used for. We came up with five factors, explaining 78% of the variance[11], which can be interpreted as *general concerns about data sharing* (General), *concerns about specific data collection and usage by the app* (Specific), *understanding about data collection and usage by the app* (Understanding), *trust towards entities involved with the app* (Trust) and *Concerns about unauthorised access to data from the app* (Unauthorised). The variables loading into each one of these factors are provided on Table 4.

Factor	Variable	Loading
General data sharing concerns (General) (higher values = lower level of concern)	General concerns over location sharing	0.91
	General concerns over proximity sharing	0.89
App-specific attitudes (Specific) (higher values = more comfortable or willing to share data)	Being comfortable with different purposes of using the app	0.89
	Being comfortable with different data collection models	0.89
	Willingness to share data from the app with different entities	0.79
	Willingness to share different types of data with the app	0.79
Understanding about the app (Understanding) (higher values = perception of more extensive data collection and use)	Number of entities one believes have access to the data from the app	0.85
	Beliefs regarding where the data is stored	0.81
	Number of data types one believes is collected by the app	0.75
	Number of activities one believes the data from the app is used for	0.67
Trust towards entities involved with the app (Trust) (higher values = willing to trust more entities)	Number of entities one is willing to trust	0.96
Concerns about unauthorised access (Unauthorised) (higher values = lower level of concern)	Concerns about unauthorised access to the app by different entities	0.91

Table 4. Factor analysis of privacy-related variables (primary loadings)

We used an ordinal regression model with partially proportional odds[12], including the factors identified above together with the variables studied in RQ1, namely, demographics (as age, gender, country and technology experience) and awareness about existing apps as predictors and privacy concerns (measured on a scale from 1 = not concerned to 4 = very concerned) as the outcome variable. We found that the factors Specific, Understanding, Trust and Unauthorised had significant

[9] All average scores were computed on items with Cronbach's $\alpha > .7$.

[10] We decided to count the number of entities instead of considering each entity separately, in order both to reduce the dimensionality of data, as well as to reflect the fact that several entities are usually involved in development and maintenance of the app, as well as its data processing.

[11] We used varimax rotation and kept factors with EV of at least 1

[12] Variables Specific, General and age were shown to violate the proportional odds assumption.

effect on privacy concerns (increasing the odds of lower privacy concern levels for higher values of Specific, Trust and Unauthorised, and increasing the odds of being "slightly concerned" versus "not concerned", as well as the odds of being "somewhat concerned" versus "slightly concerned" for higher values of Understanding), and age had a small positive effect on the odds of being "not concerned" versus "slightly concerned". Furthermore, participants from US had increased odds of higher concern level compared to people from Denmark. None of the other variables were found to be significant (see Table 5, for the analysis results for all the predictors incl. non-significant ones, see Appendix B). The post-hoc pairwise tests for the categorical predictors in the model did not reveal any further significant factors.

term	estimate	std.error	statistic	p.value
Not concerned|Slightly concerned.Specific	1.10	0.17	6.52	< 0.0001
Slightly concerned|Somewhat concerned.Specific	1.46	0.17	8.38	< 0.0001
Somewhat concerned|Very concerned.Specific	2.09	0.26	7.93	< 0.0001
Not concerned|Slightly concerned.Understanding	-0.84	0.15	-5.62	< 0.0001
Slightly concerned|Somewhat concerned.Understanding	-0.71	0.15	-4.68	< 0.0001
Not concerned|Slightly concerned.age	0.02	0.01	1.96	0.0496
countryUS	1.31	0.43	3.05	0.0023
Trust	-0.50	0.12	-4.02	< 0.0001
Unauthorised	-0.38	0.12	-3.20	0.0014

Table 5. Ordinal regression model with partially proportional odds (only significant predictors) for RQ2

Finally, we looked at how the identified factors (see Table 4) were affected by demographics. We applied linear regression to study the effect of demographic variables (age, gender, country, education, technology experience) and awareness about existing apps on each one of the factors General, Specific, Understanding, Trust, Unauthorised. We found the following significant[13] relationships:

General Participants with university education were more likely to be concerned about sharing their location and proximity information ($p = .024$).

Specific Participants from Italy were more likely than the participants from other countries to be comfortable with sharing app-specific data ($p < .0003$).

Understanding Participants with university education ($p = .036$), as well as participants aware about the existence of an app offered by the government (versus participants who were not aware about any existing apps they could use) were more likely to believe in less extensive data collection and access.

Trust Participants from Italy were likely to trust less entities in developing and maintaining the app compared to participants from Germany ($p = .0276$). Participants with more extensive technology expertise and experience were likely to trust more entities ($p = .037$).

Unauthorised Participants from the US were less likely to be concerned about unauthorised access to data from the app by diverse entities compared to participants from Italy and Germany ($p < .0001$ and $p = .0318$ respectively), and participants from Italy were more likely to be concerned compared to participants from Denmark ($p = .002$).

A summary of predictors that were found to be significant for each one of the factors is provided in Appendix B.

[13] We report the resulting p-values without adjusting for multiple comparisons of several factors.

6 DISCUSSION

The participants in our study had different attitudes and adoption behavior when it comes to C19CT apps. In particular, there were noticeable differences in terms of app adoption between our participants in the US and in Europe. These differences, however, are mostly explained by the lack of awareness by US participants about the particular apps they could install and use, as opposed to the participants from European countries, where official governmental apps were developed and widely advertised. Analyzing the results also revealed differences between the countries regarding privacy aspects of using the C19CT apps; participants from the US were the most concerned about privacy implications, but also assumed the highest level of privacy-invasiveness on behalf of the app. Participants from Europe, on the other hand, were more willing to trust governmental institutions and were more aware of the workings of the C19CT apps that are currently in use, such as the fact that the app collects Bluetooth data and that this data is mostly stored locally, with the German participants expressing the highest level of such awareness.

Similarly to previous studies outlined in Section 2 (e.g., [1, 31, 48, 52]), privacy concerns were significant factors in the adoption of C19CT apps. Perhaps surprisingly, however, our study showed that participants' general attitudes of sharing their location and proximity information did not have a significant effect on privacy concerns in terms of C19CT. On the contrary, the understanding our participants had of how the apps collect and process data, including the purposes for using such data, were shown to have the largest effect. These findings might indicate that at least some of the participants were well-aware of the fact that the widely deployed C19CT apps do not rely on collecting neither location, nor proximity information – nonetheless, the majority of the participants across all countries (from 66% in Denmark to 92% in the US) did indeed believe that the app collects users' location, among other data. Such beliefs that people think the app collects location data were also identified by Haring et al. [17] in a study conducted in Germany just before the release of the app. A perhaps more suitable explanation to our finding that general attitudes of sharing location and proximity information did no have an effect on privacy concerns related to C19CT, lies in the contextual nature of privacy [49]: people's concerns about privacy are not only based on what data is being collected, but also on a variety of other factors, including but not limited to the perceived use of the data, the entities who have access to it and whether the data is sufficiently protected against unauthorised access [3]. Framing the debate around C19CT apps as "privacy versus public health" is therefore misleading, given that people's hesitance to use such apps seems to be based not on their concerns to share data per se, but instead on concerns about the data potentially being misused.

Overall, our findings indicate that the low adoption of C19CT apps is founded in a lack of transparency and trust, as also indicated by previous studies [48]. We therefore recommend adhering to the following principles when designing and disseminating either C19CT apps or technology with a similar potential for both advancing public good or, in worst case, being misused for surveillance: First, the apps should *implement proper privacy safeguards* – a requirement that is already supported by legislation (e.g. GDPR), but that, as our study shows, is critical for the adoption of the apps. Second, the information about these safeguards has to be thoroughly *communicated* – as evidenced from our study, many participants believed the app that is available to them collects and shares more sensitive information about them than it actually does. The media of such communications as well as the extent of it (i.e. to what level of details should the workings of the app be explained) should also be studied, as communication of privacy assurances is known to be a challenge in other contexts as well [40]. Yet, our findings show that the measures for such communication provided by the respective governments at the moment of our study were not sufficient, hence, future research is needed. Potential directions of such research would be (1) identifying the "blind spots", that is, the aspects of the app functionality that have potential to create the most concerns among the users, while being the most misunderstood – for example, the belief that the app has access to location data and this data is stored either with the government or with a private company; (2) identifying and involving institutions and other entities that are trusted by the users with regards to the app usage – as evidenced from our study, such institutions can vary depending on the country, with European users being more likely e.g. to trust the governmental institutions and research facilities compared to the US users.

7 CONCLUSION

In this paper we presented a cross-country survey investigating people's adoption behavior and privacy concerns of COVID-19 contact tracing applications; we found that while people with higher level of technology expertise, and a better understanding of what data is actually collected and for what purpose, were more likely to install such app, where people with higher levels of self-defined privacy concerns were less likely to install or keep such application active. While there were interesting differences between the investigated European countries and the US, such as adoption rate, the difference likely rested in the fact that while the European countries under study saw governmental sponsored and recommended tracing apps, the US did not have any centrally recommended app.

The fight against the COVID-19 pandemic has been fought using a multitude of tools, some refer to the combination of the tools as "The Swiss Cheese"[33, 36], where each tool has weaknesses (holes in the cheese), but where all the "slices" together provide significant protection. The contact tracing applications provide just one possible layer that can be combined with many other (technical or manual) strategies. However, in many situations a technical solution might be both supplemental to manual contact tracing but also superior, for example in situations where a positive diagnosis is a sensitive issue for some people. While the contact tracing applications are not the panacea of disease prevention, it is still important to investigate the challenges of such app adoptions and provide better knowledge into how we can better design these and if they make sense to even implement for a particular population. Our study shows that a high transparency of data use, a high level of trust in the entity that releases and maintains the app are essential to adoption rates. From a broader perspective, mobile applications could provide transparency of their data use context and storage, in order to reduce privacy sensitivity, that lead to lower adoption of health essential applications such as COVID-19 contact tracing apps.

REFERENCES

[1] Samuel Altmann, Luke Milsom, Hannah Zillessen, Raffaele Blasone, Frederic Gerdon, Ruben Bach, Frauke Kreuter, Daniele Nosenzo, Séverine Toussaert, and Johannes Abeler. 2020. Acceptability of app-based contact tracing for COVID-19: Cross-country survey study. *JMIR mHealth and uHealth* 8, 8 (2020), 1–9. https://doi.org/10.2196/19857

[2] Angelo Amante and Elvira Pollina. 2020. Italians embrace coronavirus tracing app as privacy fears ease. https://www.reuters.com/article/us-health-coronavirus-italy-apps-idUSKBN23I2M5

[3] Louise Barkhuus. 2012. *The Mismeasurement of Privacy: Using Contextual Integrity to Reconsider Privacy in HCI.* Association for Computing Machinery, New York, NY, USA, 367–376. https://doi.org/10.1145/2207676.2207727

[4] Louise Barkhuus and A. Dey. 2003. Location-Based Services for Mobile Telephony: a Study of Users' Privacy Concerns. In *INTERACT.* IOS Press.

[5] Riccardo Berti, Alessandro Longo, and Simone Zanetti. 2021. Immune, what it is and how the Italian coronavirus app works. https://www.agendadigitale.eu/cultura-digitale/immuni-come-funziona-lapp-italiana-contro-il-coronavirus/

[6] Annelies G. Blom, Alexander Wenz, Carina Cornesse, Tobias Rettig, Marina Fikel, Sabine Friedel, Katja Möhring, Elias Naumann, Maximiliane Reifenscheid, and Ulrich Krieger. 2021. Barriers to the large-scale adoption of a covid-19 contact tracing app in germany: Survey study. *Journal of Medical Internet Research* 23, 3 (2021). https://doi.org/10.2196/23362

[7] Svend Brinkmann and Steinar Kvale. 2017. *The SAGE Handbook of Qualitative Research in Psychology.* Sage.

[8] A.J. Bernheim Brush, John Krumm, and James Scott. 2010. Exploring End User Preferences for Location Obfuscation, Location-Based Services, and the Value of Location. In *Proceedings of the 12th ACM International Conference on Ubiquitous Computing* (Copenhagen, Denmark) *(UbiComp '10)*. Association for Computing Machinery, New York, NY, USA, 95–104. https://doi.org/10.1145/1864349.1864381

[9] Sunny Consolvo, Ian E. Smith, Tara Matthews, Anthony LaMarca, Jason Tabert, and Pauline Powledge. 2005. *Location Disclosure to Social Relations: Why, When, & What People Want to Share.* Association for Computing Machinery, New York, NY, USA, 81–90. https://doi.org/10.1145/1054972.1054985

[10] Lisa O. Danquah, Nadia Hasham, Matthew MacFarlane, Fatu E. Conteh, Fatoma Momoh, Andrew A. Tedesco, Amara Jambai, David A. Ross, and Helen A. Weiss. 2019. Use of a mobile application for Ebola contact tracing and monitoring in northern Sierra Leone: A proof-of-concept study. *BMC Infectious Diseases* 19, 1 (2019), 1–12. https://doi.org/10.1186/s12879-019-4354-z

[11] Sara Delamont and Paul Atkinson. 2018. *The sage handbook of qualitative research ethics.* Sage.

[12] Mahmoud Elkhodr, Omar Mubin, Zainab Iftikhar, Maleeha Masood, Belal Alsinglawi, Suleman Shahid, and Fady Alnajjar. 2021. Technology, privacy, and user opinions of COVID-19 mobile apps for contact tracing: Systematic search and content analysis. *Journal of Medical Internet Research* 23, 2 (2021), 1–17. https://doi.org/10.2196/23467

[13] Victoria Fast and Daniel Schnurr. 2021. Incentivising the Adoption of COVID-19 Contact-Tracing Apps: A Randomised Controlled Online Experiment on the German Corona-Warn-App. In *Proceedings of the 2021 on Computers and People Research Conference* (Virtual Event, Germany) *(SIGMIS-CPR'21)*. Association for Computing Machinery, New York, NY, USA, 1–3. https://doi.org/10.1145/3458026.3462158

[14] Nicolai Franck. 2020. Smittestop-app [thumps-up] eller [thumps-down]: Skepsis og Kritik er Fuldt Berettiget, Men Jeg Vil Stadig bruge Den og tror Vi kan lære en masse. https://techliv.dk/smittestop-app-skepsis-og-kritik-er-fuldt-berettiget-men-jeg-vil-stadig-bruge-den-og-tror-vi-kan/

[15] GitHub. [n.d.]. Corona-warn-app. https://github.com/corona-warn-app/

[16] GitHub. 2020. After upgrade to iOS 13.6 the app is disabled and cannot be re-enabled because region is not supported. https://github.com/corona-warn-app/cwa-app-ios/issues/911

[17] Maximilian Häring, Eva Gerlitz, Christian Tiefenau, Matthew Smith, Dominik Wermke, Sascha Fahl, and Yasemin Acar. 2021. Never ever or no matter what: Investigating Adoption Intentions and Misconceptions about the Corona-Warn-App in Germany. In *Seventeenth Symposium on Usable Privacy and Security (SOUPS 2021)*. USENIX Association, 77–98. https://www.usenix.org/conference/soups2021/presentation/acar

[18] Hanna Heine. 2020. Corona-Warn-App version 1.10 comes with an integrated Contact journal. https://www.coronawarn.app/en/blog/2020-12-24-corona-warn-app-version-1-10-announcement/

[19] Hanna Heine. 2021. Corona-Warn-App version 1.12 comes with two new features. https://www.coronawarn.app/en/blog/2021-02-10-corona-warn-app-version-1-12/

[20] Janina Hoerdt. 2021. Aktuelle Zahlen und Fakten zur Corona-Warn-App. https://www.coronawarn.app/de/blog/2021-08-20-facts-and-figures/

[21] InfoData. 2020. Blog: I dati dell'app immuni sono disponibili in formato aperto ma si fermano al dettaglio regionale. https://www.infodata.ilsole24ore.com/2020/11/02/i-dati-dellapp-immuni-sono-disponibili-in-formato-aperto-ma-si-fermano-al-dettaglio-regionale/

[22] Leonie Kahnbach, Dirk Lehr, Jessica Brandenburger, Tim Mallwitz, Sophie Jent, Sandy Hannibal, Burkhardt Funk, and Monique Janneck. 2021. Quality and Adoption of COVID-19 Tracing Apps and Recommendations for Development: Systematic Interdisciplinary Review of European Apps. *Journal of Medical Internet Research* 23, 6 (2021), e27989. https://doi.org/10.2196/27989

[23] Gabriel Kaptchuk, Daniel G. Goldstein, Eszter Hargittai, Jake M. Hofman, and Elissa M. Redmiles. 2020. How good is good enough for COVID19 apps? The influence of benefits, accuracy, and privacy on willingness to adopt. *CoRR* abs/2005.04343 (2020). arXiv:2005.04343 https://arxiv.org/abs/2005.04343

[24] Tianshi Li, Camille Cobb, Jackie (Junrui) Yang, Sagar Baviskar, Yuvraj Agarwal, Beibei Li, Lujo Bauer, and Jason I. Hong. 2021. 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. *Pervasive and Mobile Computing* 75 (2021), 101439. https://doi.org/10.1016/j.pmcj.2021.101439

[25] Tianshi Li, Jackie Yang, Cori Faklaris, Jennifer King, Yuvraj Agarwal, Laura Dabbish, and Jason I. Hong. 2020. Decentralized is not risk-free: Understanding public perceptions of privacy-utility trade-offs in COVID-19 contact-tracing apps. *CoRR* abs/2005.11957 (2020). arXiv:2005.11957 https://arxiv.org/abs/2005.11957

[26] Xi Lu, Tera L. Reynolds, Eunkyung Jo, Hwajung Hong, Xinru Page, Yunan Chen, and Daniel A. Epstein. 2021. *Comparing Perspectives Around Human and Technology Support for Contact Tracing.* Association for Computing Machinery, New York, NY, USA. https://doi.org/10.1145/3411764.3445669

[27] C. Mancini, L. Jedrzejczyk, A. Bandara, B. Nuseibeh, K. Thomas, B. Price, Yvonne Rogers, and A. Joinson. 2010. Predators and Prey: Ubiquitous Tracking, Privacy and the Social Contract.

[28] Lauren Maytin, Jason Maytin, Priya Agarwal, Anna Krenitsky, Jo Ann Krenitsky, and Robert S. Epstein. 2021. Attitudes and perceptions toward covid-19 digital surveillance: Survey of young adults in the United State. *JMIR Formative Research* 5, 1 (2021). https://doi.org/10.2196/23000

[29] Hannah Murphy, Lauren Keahey, Emma Bennett, Archie Drake, Samantha K. Brooks, and G. James Rubin. 2020. Millennial attitudes towards sharing mobile phone location data with health agencies: a qualitative study. *Information, Communication & Society* 0, 0 (2020), 1–14. https://doi.org/10.1080/1369118X.2020.1753798 arXiv:https://doi.org/10.1080/1369118X.2020.1753798

[30] Andreas Oldeweme, Julian Märtins, Daniel Westmattelmann, and Gerhard Schewe. 2021. The role of transparency, trust, and social influence on uncertainty reduction in times of pandemics: Empirical study on the adoption of COVID-19 tracing apps. *Journal of Medical Internet Research* 23, 2 (2021). https://doi.org/10.2196/25893

[31] Esli Osmanlliu, Edmond Rafie, Sylvain Bédard, Jesseca Paquette, Genevieve Gore, and Marie-Pascale Pomey. 2021. Considerations for the Design and Implementation of COVID-19 Contact Tracing Apps: Scoping Review. *JMIR mHealth and uHealth* 9, 6 (2021). https://doi.org/10.2196/27102

[32] Kiemute Oyibo, Kirti Sundar Sahu, Arlene Oetomo, and Plinio Pelegrini Morita. 2021. Factors Influencing the Adoption of Contact Tracing Applications: Protocol for a Systematic Review. *JMIR Research Protocols* 10, 6 (2021), e28961. https://doi.org/10.2196/28961

[33] James Reason. 1990. The contribution of latent human failures to the breakdown of complex systems. *Philosophical Transactions of the Royal Society of London. B, Biological Sciences* 327, 1241 (1990), 475–484.

[34] Reuters. 2020. Italy launches COVID-19 contact-tracing app amid privacy concerns. https://www.reuters.com/article/us-health-coronavirus-italy-app-idUSKBN2383EW

[35] Robert Koch Institute. 2021. Corona-Warn-App Open Source Project. https://www.coronawarn.app/en/ last accessed on September 10th, 2021.

[36] Siobhan Roberts. 2020. The Swiss Cheese Model of Pandemic Defense. *The New York Times* (December 2020). https://www.nytimes.com/2020/12/05/health/coronavirus-swiss-cheese-infection-mackay.html?smid=url-share

[37] Frantz Rowe, Ojelanki Ngwenyama, and Jean-Loup Richet. 2020. Contact-tracing apps and alienation in the age of COVID-19. *European Journal of Information Systems* 29, 5 (2020), 545–562. https://doi.org/10.1080/0960085X.2020.1803155 arXiv:https://doi.org/10.1080/0960085X.2020.1803155

[38] Lorenzo Ruffino. 2021. Tutti i dati su immuni. https://www.youtrend.it/2020/11/24/tutti-i-dati-su-immuni/

[39] Mia Sato. 2021. Contact tracing apps now cover nearly half of america. it's not too late to use one. https://www.technologyreview.com/2020/12/14/1014426/covid-california-contact-tracing-app-america-states/

[40] Florian Schaub, Rebecca Balebako, Adam L Durity, and Lorrie Faith Cranor. 2015. A design space for effective privacy notices. In *Eleventh symposium on usable privacy and security (SOUPS 2015)*. 1–17.

[41] Emily Schildt, Martin Leinfors, and Louise Barkhuus. 2016. Communication, coordination and awareness around continuous location sharing. *Proceedings of the International ACM SIGGROUP Conference on Supporting Group Work* 13-16-Nove (2016), 257–265. https://doi.org/10.1145/2957276.2957289

[42] John S. Seberger and Sameer Patil. 2021. Us and Them (and It): Social Orientation, Privacy Concerns, and Expected Use of Pandemic-Tracking Apps in the United States. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems* (Yokohama, Japan) *(CHI '21)*. Association for Computing Machinery, New York, NY, USA, Article 65, 19 pages. https://doi.org/10.1145/3411764.3445485

[43] Emily Seto, Priyanka Challa, and Patrick Ware. 2021. Adoption of COVID-19 contact tracing apps: A balance between privacy and effectiveness. *Journal of Medical Internet Research* 23, 3 (2021), 1–7. https://doi.org/10.2196/25726

[44] smittestop.dk. [n.d.]. Processing of Personal Data. https://smittestop.dk/en/data-protection/

[45] Henrik Søe. 2020. Fejl I smittestop-app: Brugere har misset advarsler. https://www.avisen.dk/citat-erkender-fejl-android-brugere-har-misset-smi_627068.aspx

[46] Karen P. Tang, Jialiu Lin, Jason I. Hong, Daniel P. Siewiorek, and Norman Sadeh. 2010. Rethinking Location Sharing: Exploring the Implications of Social-Driven vs. Purpose-Driven Location Sharing. In *Proceedings of the 12th ACM International Conference on Ubiquitous Computing* (Copenhagen, Denmark) *(UbiComp '10)*. Association for Computing Machinery, New York, NY, USA, 85–94. https://doi.org/10.1145/1864349.1864363

[47] Rae Thomas, Zoe A Michaleff, Hannah Greenwood, Eman Abukmail, and Paul Glasziou. 2020. More than privacy: Australians' concerns and misconceptions about the COVIDSafe App. *medRxiv* (2020). https://doi.org/10.1101/2020.06.09.20126110 arXiv:https://www.medrxiv.org/content/early/2020/07/29/2020.06.09.20126110.full.pdf

[48] Christine Utz, Steffen Becker, Theodor Schnitzler, Florian M. Farke, Franziska Herbert, Leonie Schaewitz, Martin Degeling, and Markus Dürmuth. 2021. *Apps Against the Spread: Privacy Implications and User Acceptance of COVID-19-Related Smartphone Apps on Three Continents*. Association for Computing Machinery, New York, NY, USA. https://doi.org/10.1145/3411764.3445517

[49] Jessica Vitak and Michael Zimmer. 2020. More Than Just Privacy: Using Contextual Integrity to Evaluate the Long-Term Risks from COVID-19 Surveillance Technologies. *Social Media + Society* 6, 3 (2020), 2056305120948250. https:

//doi.org/10.1177/2056305120948250 arXiv:https://doi.org/10.1177/2056305120948250 PMID: 34192036.

[50] Viktor von Wyl, Marc Höglinger, Chloé Sieber, Marco Kaufmann, André Moser, Miquel Serra-Burriel, Tala Ballouz, Dominik Menges, Anja Frei, and Milo Alan Puhan. 2021. Drivers of Acceptance of COVID-19 Proximity Tracing Apps in Switzerland: Panel Survey Analysis. *JMIR Public Health Surveill* 7, 1 (6 Jan 2021), e25701. https://doi.org/10.2196/25701

[51] Baobao Zhang, Sarah Kreps, and Nina McMurry. 2020. Americans' perceptions of privacy and surveillance in the COVID-19 Pandemic. (05 2020). https://doi.org/10.31219/osf.io/9wz3y

[52] Bettina Maria Zimmermann, Amelia Fiske, Barbara Prainsack, Nora Hangel, Stuart McLennan, and Alena Buyx. 2021. Early perceptions of COVID-19 contact tracing apps in German-speaking countries: Comparative mixed methods study. *Journal of Medical Internet Research* 23, 2 (2021), 1–17. https://doi.org/10.2196/25525

A QUESTIONNAIRE

See the file included with the supplementary materials.

B STATISTICAL MODELS

We provide the output of the statistical model used for RQ2, namely, the analysis of deviance for the logistic regression model with the users decision to install the app as an outcome[14]. We provide the output of the statistical model used for RQ3, namely, (1) the output of the ordinal regression model with partially proportionate odds and the post-hoc analyses of categorical variables of more than two levels[15], and (2) the results of the analysis of variance for each one of the factors *Specific*, *General*, *Understanding*, *Trust* and *Unauthorised* as response variables, and the results of pairwise post-hoc comparisons for the categorical predictors found to have a significant effect.

	LR Chisq	Df	Pr(>Chisq)
country	1.43	3	0.6996
gender	4.91	2	0.0860
age	1.42	1	0.2328
university	4.88	1	0.0271
technology_aggr	8.11	1	0.0044
awareness	12.03	1	0.0005
privacy_concerns	22.64	1	< 0.0001
trust	1.19	1	0.2753
purposes	9.06	1	0.0026

Table 6. Analysis of deviance for the logistic regression model for RQ2

Received February 2022; revised May 2022; accepted June 2022

[14] Note, in the evaluation of RQ2, the "awareness" variable only had to levels, excluding six "other, please specify" answers

[15] Due to low number of participants who reported their gender as non-binary, we did not conduct post-hoc tests on the "gender" variable

term	estimate	std.error	statistic	p.value
Not concerned|Slightly concerned.(Intercept)	-0.91	1.27	-0.72	0.4735
Slightly concerned|Somewhat concerned.(Intercept)	0.83	1.28	0.65	0.5154
Somewhat concerned|Very concerned.(Intercept)	4.29	1.39	3.09	0.002
Not concerned|Slightly concerned.Specific	1.10	0.17	6.52	< 0.0001
Slightly concerned|Somewhat concerned.Specific	1.46	0.17	8.38	< 0.0001
Somewhat concerned|Very concerned.Specific	2.09	0.26	7.93	< 0.0001
Not concerned|Slightly concerned.Understanding	-0.84	0.15	-5.62	< 0.0001
Slightly concerned|Somewhat concerned.Understanding	-0.71	0.15	-4.68	< 0.0001
Somewhat concerned|Very concerned.Understanding	-0.33	0.22	-1.49	0.1363
Not concerned|Slightly concerned.age	0.02	0.01	1.96	0.0496
Slightly concerned|Somewhat concerned.age	0.02	0.01	1.72	0.085
Somewhat concerned|Very concerned.age	-0.01	0.02	-0.70	0.4809
countryDE	0.58	0.33	1.78	0.0745
countryIT	0.50	0.34	1.48	0.1392
countryUS	1.31	0.43	3.05	0.0023
genderMale	0.18	0.22	0.80	0.4213
genderNon-binary	0.49	1.47	0.34	0.7357
universityTRUE	0.11	0.23	0.47	0.6375
technology_aggr	-0.02	0.12	-0.15	0.8772
awarenessNoAvailableApps	0.19	0.46	0.42	0.674
awarenessOfficialApp	-0.08	0.49	-0.16	0.8744
General	0.00	0.11	0.02	0.9871
Trust	-0.50	0.12	-4.02	< 0.0001
Unauthorised	-0.38	0.12	-3.20	0.0014

Table 7. Ordinal logistic regression model for RQ3

contrast	estimate	SE	df	z.ratio	p.value
DK - DE	-0.5806	0.3255	Inf	-1.784	0.2811
DK - IT	-0.4999	0.3381	Inf	-1.479	0.4504
DK - US	-1.3129	0.4302	Inf	-3.052	0.0122
DE - IT	0.0807	0.2997	Inf	0.269	0.9932
DE - US	-0.7322	0.4215	Inf	-1.737	0.3043
IT - US	-0.8130	0.4526	Inf	-1.796	0.2750

Table 8. Post-hoc tests for RQ3 (country)

contrast	estimate	SE	df	z.ratio	p.value
no awareness about official app - no awareness about any available apps	-0.1944	0.4621	Inf	-0.421	0.9071
no awareness about official app - awareness about official app	0.0773	0.4887	Inf	0.158	0.9863
no awareness about any available apps - awareness about official app	0.2716	0.3701	Inf	0.734	0.7434

Table 9. Post-hoc tests for RQ3 (awareness)

	Df	Sum Sq	Mean Sq	F value	Pr(>F)
country	3	43.60	14.53	16.49	<.0001
gender	2	1.58	0.79	0.90	0.4094
age	1	0.31	0.31	0.35	0.5520
university	1	0.10	0.10	0.11	0.7425
technology_aggr	1	2.16	2.16	2.45	0.1186
awareness	2	2.05	1.03	1.17	0.3128
Residuals	375	330.45	0.88		

Table 10. Analysis of variance for the factor *Specific*

contrast	estimate	SE	df	t.ratio	p.value
DK - DE	-0.0190	0.1442	375	-0.132	0.9992
DK - IT	-0.5912	0.1414	375	-4.180	0.0002
DK - US	0.2389	0.1917	375	1.246	0.5977
DE - IT	-0.5722	0.1313	375	-4.356	0.0001
DE - US	0.2579	0.1955	375	1.319	0.5514
IT - US	0.8300	0.1987	375	4.176	0.0002

Table 11. Post-hoc tests for the factor *Specific*

	Df	Sum Sq	Mean Sq	F value	Pr(>F)
country	3	7.58	2.53	2.59	0.0523
gender	2	0.51	0.25	0.26	0.7713
age	1	1.71	1.71	1.76	0.1859
university	1	4.95	4.95	5.08	0.0248
technology_aggr	1	2.09	2.09	2.15	0.1437
awareness	2	1.71	0.86	0.88	0.4158
Residuals	375	365.39	0.97		

Table 12. Analysis of variance for the factor *General*

	Df	Sum Sq	Mean Sq	F value	Pr(>F)
country	3	23.25	7.75	8.46	0.0000
gender	2	2.64	1.32	1.44	0.2377
age	1	0.28	0.28	0.30	0.5839
university	1	4.22	4.22	4.61	0.0324
technology_aggr	1	0.88	0.88	0.97	0.3262
awareness	2	7.24	3.62	3.95	0.0200
Residuals	375	343.32	0.92		

Table 13. Analysis of variance for the factor *Understanding*

contrast	estimate	SE	df	t.ratio	p.value
DK - DE	0.0172	0.1470	375	0.117	0.9994
DK - IT	-0.2012	0.1441	375	-1.396	0.5029
DK - US	-0.2795	0.1954	375	-1.431	0.4810
DE - IT	-0.2184	0.1339	375	-1.631	0.3623
DE - US	-0.2967	0.1993	375	-1.489	0.4451
IT - US	-0.0783	0.2026	375	-0.387	0.9803

Table 14. Post-hoc tests for the factor *Understanding* (country)

contrast	estimate	SE	df	t.ratio	p.value
no awareness about official app - no awareness about any available apps	-0.0203	0.2141	375	-0.095	0.9951
no awareness about official app - awareness about official app	0.4451	0.2326	375	1.914	0.1361
no awareness about any available apps - awareness about official app	0.4654	0.1711	375	2.719	0.0187

Table 15. Post-hoc tests for the factor *Understanding* (awareness)

	Df	Sum Sq	Mean Sq	F value	Pr(>F)
country	3	23.04	7.68	8.18	0.0000
gender	2	1.23	0.62	0.66	0.5190
age	1	0.33	0.33	0.35	0.5523
university	1	0.20	0.20	0.22	0.6424
technology_aggr	1	4.93	4.93	5.25	0.0225
awareness	2	3.74	1.87	1.99	0.1381
Residuals	375	351.98	0.94		

Table 16. Analysis of variance for the factor *Trust*

contrast	estimate	SE	df	t.ratio	p.value
DK - DE	-0.1644	0.1488	375	-1.105	0.6867
DK - IT	0.2148	0.1459	375	1.472	0.4556
DK - US	0.2086	0.1978	375	1.054	0.7174
DE - IT	0.3792	0.1356	375	2.798	0.0276
DE - US	0.3730	0.2018	375	1.849	0.2522
IT - US	-0.0062	0.2051	375	-0.030	1.0000

Table 17. Post-hoc tests for the factor *Trust*

	Df	Sum Sq	Mean Sq	F value	Pr(>F)
country	3	25.72	8.57	9.23	0.0000
gender	2	4.50	2.25	2.42	0.0902
age	1	1.31	1.31	1.41	0.2353
university	1	0.68	0.68	0.73	0.3940
technology_aggr	1	1.08	1.08	1.17	0.2807
awareness	2	2.92	1.46	1.57	0.2088
Residuals	375	348.32	0.93		

Table 18. Analysis of variance for the factor *Unauthorised*

contrast	estimate	SE	df	t.ratio	p.value
DK - DE	0.1691	0.1480	375	1.142	0.6635
DK - IT	0.5144	0.1452	375	3.543	0.0025
DK - US	-0.3824	0.1968	375	-1.943	0.2118
DE - IT	0.3453	0.1348	375	2.560	0.0527
DE - US	-0.5515	0.2007	375	-2.748	0.0318
IT - US	-0.8968	0.2040	375	-4.395	0.0001

Table 19. Post-hoc tests for the factor *Unauthorised*