Privacy Research on the Pulse of Time: COVID-19 Contact-Tracing Apps

Eva Gerlitz and Maximilian Häring

1 Introduction

In 2020, COVID-19 hit the World, and with it came the desire for a well-functioning and a fast-working possibility to trace contacts of those people who tested positive for the virus, a method called *contact tracing*.

> **Definition: Contact Tracing**
> Following the Cambridge Dictionary, contact tracing is "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" [8]. Similar definitions are used elsewhere, e.g., by the World Health Organization (WHO) [11] and the European Centre for Disease Prevention and Control (ECDC) [9].

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 [12]. It has several advantages compared to a manual approach done

Authors are listed in alphabetical order and contributed equally

E. Gerlitz
Fraunhofer FKIE, Bonn, Germany
e-mail: gerlitz@cs.uni-bonn.de

M. Häring (✉)
Universität Bonn, Institut für Informatik, Bonn, Germany
e-mail: haering@cs.uni-bonn.de

N. Gerber et al. (eds.), *Human Factors in Privacy Research*,
https://doi.org/10.1007/978-3-031-28643-8_11

by health workers, e.g., that it enables to warn more people who else could not have been notified due to incomplete memory or knowledge about contacts of an infected person. Digital contact tracing also supports the authorities by 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 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 [33].

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 a contact with someone who is infected with the virus [7]. Many other governments followed, and a lot of those contact tracing apps (CTA) based their tracing on Bluetooth or the users' location. As of March 2021, the MIT Technology Review lists 49 contact tracing apps in 48 countries from around the World [1] and an overview from Google lists 60 apps that make use of their provided framework [27].

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. 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 case for apps that should technically prevent abuse [10].

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 [17]. 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 [24].

Taken together, these requirements (privacy preserving and the need to reach a large part of the population) were able to influence political decisions, e.g., in Germany [6], where the government switched to a more privacy-preserving app after another one had already been planned.

The concerns for misuse of the captured data were, in fact, not unfounded: Later, in at least one case in Germany, data of a private app that was used to check-in into restaurants and that stored the data centrally were used by the criminal investigation department to find witnesses of an accident. This happened even though it is illegal to use these data for law enforcement purposes, according to the Infection Protection Act for reasons of data protection [22].

In Singapore, data captured through the widespread contact tracing app "Trace-Together," about which it was claimed after its release that the data would only be accessed if a user tests positive for COVID-19, were used in a murder investigation [32].

So, privacy has been a big topic in the development and the public discussions centered around contact tracing apps. But how big of a role does and did privacy actually play in the mind of potential users when they needed to decide whether or not to install a contact tracing app? And what can privacy research learn from that?

This chapter is a starting point for every reader interested in these questions. In this chapter, we:

- Give a brief outline of the tracing technologies and their implications for the users' data and therefore privacy.
- Look at scientific studies with end users and how their privacy concerns impacted their decision to install a contact tracing app.
- Set the study results in the context of the used methodology (e.g., the time the study was conducted or who was asked).

After reading this chapter, the reader will have an overview of the general privacy discussion on contact tracing apps in the context of COVID-19 and hints on where to find further information.

2 Tracing Technologies

This section gives a brief overview of technical possibilities to automatically warn people who had been in contact with someone who later tests positive for COVID-19. Worldwide, different versions of contact tracing apps were proposed, discussed, and rolled out. 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 [25]) to functioning as access control (e.g., in China [23]).

Obviously, it is (currently) not feasible to technically directly track whether a person met another person; therefore, many solutions use the personal smartphone as a proxy. The apps capture whether a device was in proximity to another device, therefore 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 encountered 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 for the reader to have a general overview and can follow the debates around the different apps, their approaches, and possible implications for the users. Please note that this is not a complete list of technologies.

2.1 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. [18], 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 [15]), 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 privacy in the contact tracing context, one has to look at the storage location of the logged contact data and the usage of Bluetooth Low Energy (LE). It works 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 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 an infected person, the approach is called *decentral*. On the other hand, *central* means that the devices 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 hosting or having access to the service (e.g., the government) could gain access to the data [28]. In this case, the third party 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. [5].

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., [4, 5, 14, 26, 29]).

2.2 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 the contacts of an infected person 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 are available.

3 Privacy and Contact Tracing Apps—User Studies

The previous sections concerned technical circumstances to give the reader an overview of the situation. This section now focuses on the end user, thus the person owning a smartphone, and who is the potential user of an app. We give insight into what the studied participants think about contact tracing apps in terms of privacy, and how privacy considerations impact the willingness to use such apps.

For this, we conducted a literature review. In 2020, the topic of contact tracing apps was highly relevant and design decisions needed to be made urgently, so many researchers around the world examined the effect of different app properties and their general acceptance in the public population: The ACM Digital Library [2], for example, as of September 2022, lists around 32K publications published since 2020 when searching for "contact tracing."

We thus specified our search term such that the terms "contact," "trac*," and "priv*" had to be found in either the title or the abstract. Our full search comprised the databases ACM Digital Library [2], IEEE Xplore [19], and Web of Science [38]. We also analyzed the Google Scholar top twenty security conferences and journals if their names included "privacy" and the A* and A CORE-ranked privacy conferences and journals. Only those that were not already included in the previous database search underwent a manual title search. This included the Symposium On Usable Privacy and Security (SOUPS) and the International Conference on Security and Privacy for Communication Networks (SecureComm).

After this search, we ended up with 245 papers. We manually reviewed all abstracts and only picked those that fit our requirements. Articles were excluded if they matched the following criteria:

- Not related to contact tracing technology to combat COVID-19.
- No user study was conducted. (This included all studies that looked at user feedback from the App stores of Apple or Google.)
- The user study did not look at sentiments of users concerning the privacy aspects of contact tracing apps.

We ended up with 13 papers that are covered in this chapter. Table 1 gives a brief overview of the included studies.

It must be noted that because of the urgency and its possible high relevance to ongoing discussions, many studies were not only published in a peer-reviewed conference or journal but faster published, e.g., by uploading on arXiv. Those are not necessarily of bad quality but have to be read more carefully than work that was

Table 1 Brief overview of the presented studies. If a specific contact tracing app was investigated, this information is included in brackets

Authors	Country	*n*	Purpose of the app (CT = Contact tracing)	Used standardized questionnaire?
Huang et al. [18]	USA	44	CT, Home quarantine, Epidemiological investigation support system, Information tracking of dine-in customers, E-permit service	No
Häring et al. [16]	Germany	744	CT (CWA)	No
Utz et al. [37]	Germany, USA, China	1003, 1003, 1019	CT, Symptom Check, Quarantine Enf., Information, Health Certificate	IUIPC, 2004
Redmiles et al. [28]	USA	1000	CT, Information	No
Xie et al. [39]	Ireland	286	CT (COVID Tracker)	Westin's privacy segmentation index (PSI), privacy attitude questionnaire (PAQ)
Trestian et al. [36]	Ireland	258	CT (COVID Tracker)	Westin's privacy segmentation index (PSI)
Lu et al. [21]	USA	291	CT (identifying and notifying close contacts) + monitoring symptoms	No
Dooley et al. [13]	USA	7,010,271 impressions	CT	–
Zampedri et al. [40]	Belgium	15	CT	No
Sharma et al. [30]	27 different countries	261	CT, information, self-assessment	No
Trestian et al. [35]	Ireland	1001	CT (COVID Tracker)	Westin's privacy segmentation index (PSI)
Jamieson et al. [20]	USA	290	CT	UTAUT
Aji et al. [3]	Malaysia	505	CT (MySejahtera)	No

already peer-reviewed. For this reason, we only include peer-reviewed work in this chapter but would like to point out that many (in our sample of papers 9) of those cite such publications. Also, we want to point out to the reader that the studies were not conducted in the same setting: Some asked about a hypothetical app, others studied an existing app, and others an app that was about to be published. Additionally, the design of the presented apps differed, making the comparison additionally hard.

When presenting the results of a paper, we will clarify what app was examined throughout the study.

3.1 Results from User Studies—Privacy Concerns

This section presents the privacy concerns participants had or mentioned in user studies. Following our goal, we will only describe the privacy-relevant questions for each paper. Please note that the studies use a concept "privacy" that not always means the same thing, e.g., the PSI (privacy segmentation index) or a direct question about privacy concerns.

Although timed differently and with different local effects, there were some very similar progression steps of the pandemic worldwide. The following publications are thus sorted by the date the reported studies were started, so that the reader is able to set them into context of the situation at that time.

Some of the presented studies did not solely concentrate on contact tracing but also included other purposes of COVID-19 apps, such as symptom checks or providing information about the current COVID-19 situation. An overview of the apps that were included is given in Table 1. We want to note that we will not report statistical results in detail, as this would come with the need of a detailed description of the used tests. Instead, if the publication mentions a statistically significant test, we report that.

Huang et al. [18] conducted 44 interviews concerning six made-up information-tracking solutions that were based on existing apps. Those were not just contact tracing apps but also apps to, e.g., monitor quarantine. The participants were asked about their perceptions of the different solutions. The interviews were conducted between May 12, 2020, and January 4, 2021. Regarding privacy, participants expressed concerns about the data used (e.g., selfies and location data), data that might be collected undocumented, the long-term misuse of personal data, and further usage, such as unauthorized sharing. Among others, threats like identifying theft or data breach were mentioned.

Häring et al. [16] conducted a survey study in June 2020 in Germany, right before the official German contact tracing app, the Corona-Warn-App (CWA), was published. The 744 participants were asked what attributes of the soon-to-be-released app were true, and whether they would use the app. The authors also asked the participants to rate the influence of potential properties. They found that over a fourth of the participants believed the app would threaten their privacy. Six of the potential properties could be attributed to a centralized approach. The authors saw that those properties that would be beneficial to the user or society in general (e.g., allowing a better assessment of the situation or allowing the official health institute to see contacts in order to warn contacts) statistically positively impacted the intention to install the app, whereas those that focus on the potential disadvantages (e.g., Health officials seeing distance violations) statistically impacted the intention negatively.

Utz et al. [37] surveyed people in Germany, the USA, and China. The surveys were conducted between June and August 2020. They presented their participants' ten different hypothetical COVID-19 apps and then asked them to rate the apps based on different criteria. The apps were built using the following properties (among others): data collected, user anonymity, data receiver, and data transmission. The participants were also asked for general negative and positive reasons why they would or would not install a contact tracing app. After that, they filled the Internet Users' Information Privacy Concerns (IUIPC, 2004) constructs (see also the chapter "Toward Valid and Reliable Privacy Concern Scales: The Example of IUIPC-8"). The authors found that 40% of the participants reported being generally concerned about their privacy regarding contact tracing apps. Participants from Germany who had high concerns regarding data collection (IUIPC: Collection) were significantly less likely to use any app.

Redmiles et al. [28] surveyed 1000 US Americans in June 2020 about specific privacy concerns of COVID-19 apps. Forty-eight percent were concerned about someone being able to learn their location information, and 31% feared someone could find out who they have been in contact with. Thirty-six percent were not concerned about any of the presented possible concerns.

Sharma et al. [30] distributed a survey from July to August 2020 on social media and community groups. The survey was conducted in English, and they gathered 261 complete responses from 27 countries. They found that the participants' privacy concerns were about data privacy and data practices.

Xie et al. [39] and Trestian et al. [36] report the results from a survey pilot study ($n = 286$ [39], $n = 258$ [36]) that was open for one month from August 27, 2020, on. The full study that was conducted between November 2020 and January 2021 with 1001 participants is reported by Trestian et al. [35]. They made use of the PSI (privacy segmentation index) to check for connections between privacy attitudes and installation willingness. All three papers found that participants who identified as privacy fundamentalists, a category of the PSI, were least willing to share their personal data with a contact tracing app.

Lu et al. [21] did not only investigate contact tracing apps but compared them to human contact tracers. For this, they surveyed 291 Americans in August 2020. They asked how comfortable they would be with an app or a human to identify close contacts, be notified as a contact, and share a daily health status. The percentage of participants who reported being very comfortable or comfortable with each approach was in the range of 50.1–69.5%. There was no overall difference between human and digital contact tracing. However, the authors found an interaction effect: Participants were significantly more comfortable using digital tracing for monitoring their daily health status. In an open-ended question, the authors also wanted to know about benefits and risks of digital and human contact tracing. The results indicate that digital contact tracing could, in fact, also have perceived privacy benefits: Participants mentioned that technology could allow for anonymity, avoid being judged, and might also not bring up social anxiety when dealing with sensitive health topics. Finally, the authors asked for the participants' willingness to share different types of personal information typically collected by one or both contact tracing approaches. For this question, they saw that participants were still significantly more comfortable sharing data with human contact tracers. The concern to share data with digital contact tracing was often related to concerns related to data security.

Dooley et al. [13] conducted an experiment in Louisiana in February 2021. In this, they tested different advertisements for Louisiana's COVID-19 exposure-notification app. In the advertisements, they included a collective or individual benefit of the app and different nuances of privacy and data collection transparency. The authors then analyzed the proportion of people who clicked on the advertisement. They found that data collection and privacy transparency have different impacts, depending on the appeal (collective or individual). Ads with a collective appeal perform better when paired with privacy transparency statements but worse with data transparency statements. A data transparency statement increased the number of clicks for ads that point to an individual benefit, whereas a technical privacy statement decreased this number. In their discussion, the authors assume that combining a collective benefit with information about individual data that is collected might conflict with peoples' sense of collectivist purpose.

3.2 Influence of Privacy on Using a CTA

In this section, we summarize findings that bring privacy considerations and the users' intention to use a contact tracing app together, answering the question how they relate and whether concerns affect the intention to install.

First of all, it was reported that **only a few participants have concerns** about their privacy in the context of contact tracing in general: Lu et al. [21] found 6.5% of their participants not to be comfortable with contact tracing in general, no matter if done by a human or digitally. Many of them (4% of all participants) explicitly mentioned privacy as the reason for this.

However, when specifically asking about contact tracing apps, the feelings seem to shift. Thus, studies found an **influence of privacy concerns on the willingness to install** a contact tracing app: Häring et al. [16] saw that the general concern that the app threatens one's privacy and the belief that the government would be able to see distance violations significantly influenced the willingness to use the app negatively. Utz et al. [37] saw that German participants were less likely to use an app if the data would be transferred to private companies, law enforcement, or the general public. They also found that participants with "higher privacy concern with regard to data collection practices (IUIPC (2004): Collection)" were significantly less likely to install an app. In an interview study with 15 participants, Zampedri [40] found that many of those who did not download the Belgian contact tracing app worry about privacy violations and lack of data transparency. Even though the Belgian app followed the decentralized approach, the participants believed the app to be privacy-invasive and that the government had access to the data. Huang et al. [18] found that privacy concerns are associated "with participants' unwillingness to adopt the solutions". In a study by Sharma et al. [30], 25% of the participants mentioned that a privacy breach would be a reason to uninstall the app. Yet, if a government forces their citizens to use an app, privacy concerns seem to be overruled: Aji et al. [3] conducted a survey in Malaysia with 505 participants who were users of the Malaysian official contact tracing app. This app asks for personal information, such as the telephone number and the name, and can be used to check-in to places the user is visiting. The authors were interested in the participants' data usage and privacy awareness about the app. They saw that in general, most participants were aware of issues the app had, e.g., that the government has access to the user's location and personal information when using the app.

So while privacy concerns seem to be an influencing factor for not installing a contact tracing app, **the opposite does not seem to apply**. Having no privacy concerns did not necessarily lead people to install an app, as Jamieson et al. [20] found. They saw that being unconcerned about privacy or data leakage was not enough to actually motivate people to install a contact tracing app. However, other motivations were needed, such as providing evidence of the app's effectiveness in protecting members of one's community. The implementation of an app thus seems to be just one part of the story.

4 Privacy: A Matter of Asking? Looking at Different Methods

In this section, we want to give an overview of how the different aspects of the chosen methodology could have impacted the results. While some of these aspects cannot always be prevented, they should be kept in mind when evaluating the results.

We would like to point out that most of the following methodological aspects apply to almost any study conducted with humans but might take on different dimensions, depending on the subject that is studied. We discuss aspects in the context of contact tracing apps that also apply to other research areas.

4.1 Timing and Context

Since the topic of contact tracing apps was urgent and relatively new, all studies presented in this chapter are cross-sectional studies and not longitudinal studies, which means that users' sentiments and concerns were only captured at one specific time. Some of the presented studies are more than two years old, and replications are missing in this set of publications.

With this, overall societal attitudes can have more impact on the data than what would be seen if looking at a topic at several times. For contact tracing apps in particular, there could be a difference in attitudes depending on whether an app is already published for some time without any major issues reported or whether an app is still in the implementation phase and several details are not known yet. Apart from that, public discussion could influence the feeling toward technology. Some of these topics could also be seen in the publications:

Privacy Concerns Might Be Overruled by Extreme Situations Trestian et al. [35] investigated the privacy paradox of contact tracing apps. This paradox refers to the discrepancy between expressed privacy concerns and actual behavior. The authors surveyed Irish citizens and classified them into three privacy groups according to the Privacy Segmentation Index (PSI) (privacy fundamentalists, pragmatics, and unconcerned). To analyze the privacy paradox, they asked the participants whether they would be willing to share their mobile data (a) to help defeat COVID-19 and (b) in normal circumstances. They found that in all privacy groups, more participants are willing to share their data in the context of COVID-19: Looking at all participants combined, the percentage rose from 14% for those who would normally share their data to 61% for fighting COVID-19. Still, the numbers depend on the PSI: Participants classified as "privacy fundamentalists" were less willing to share compared to those who were classified as "unconcerned" [39]. The authors also found that of those who use the app (55% of 258), 18% mentioned privacy concerns, and 26% thought it could be used for surveillance [36]. Sharma et al. [30] reported as a typical response to why the participants installed the app that they were not concerned about their privacy and that other aspects, such as "a sense of responsibility," were more important.

Political Enforcement's or the Provider's Role in Decision-Making Aji et al. [3] conducted their survey in Malaysia and found that most participants were aware of issues the app had (e.g., access of the government to user's location and personal information). Yet, in Malaysia, citizens could be punished if not using the app and the authors conclude that privacy concerns seem to be overruled by the enforcement issued by the government.

Sharma et al. [30] report that trust in the provider plays an important role in the adoption and that privacy benchmarks and transparency in data policy are not enough, if the data are not handled by a trusted entity. For the global North, the authors found that over 50% of the participants believed that university research groups and healthcare providers would protect the collected data. On the other hand, over 50% did not put this amount of trust into industry startups and large corporations. The importance of the provider was also emphasized by Huang et al. [18]. They found that "most participants were very comfortable with the health authorities and the government as the solution provider."

Intention–Behavior Gap Third, people do not always follow what they intend to do, known as intention–behavior gap [31] (see also the chapter "From the Privacy Calculus to Crossing the Rubicon: An Introduction to Theoretical Models of User Privacy Behavior"). Jamieson et al. [20] examined this in the context of contact tracing apps by conducting a study among 290 Americans who were presented with a hypothetical app. Depending on the state the participants lived in, they were separated into those who had access to a contact tracing app and those who did not. They found that while privacy concerns influenced people's stated intention to install a contact tracing app, privacy was no longer an influential factor for installing an app. It seems that other considerations became more important.

4.2 Who Is Asked?

The participants and thus the recruitment can have a strong influence on the results. In the following, we will summarize what we found in the literature to have an effect on the results in the context of CTA.

Personal views on topics can influence how properties related to them are seen: Häring et al. [16] presented potential properties the CWA could have. One of them proposed that the RKI,[1] would see that users are not keeping a minimal distance to each other. If this were true, it would, in fact, be a problem for the users' privacy. When the participants were asked how this property would influence their decision to install or not install the app, the authors saw that 25% of the people who were very certain about their installation decision ("I will definitely install the app") would reconsider if this property were true. When looking at the group of participants who were not so certain ("I will probably install the app"), the number of participants who indicated not to like this property went up to 35%. This general tendency should be considered when recruiting participants or interpreting the results.

Cultural Differences Utz et al. [37], who conducted the same survey in Germany, USA, and China, found that participants from China were much more open to installing a contact tracing app in general, compared to the other countries, even when those have real consequences for the users' freedom, such as quarantine enforcement. When asked for general negative aspects of contact tracing apps, 37.5% of the Chinese participants mentioned either something positive or stated that they do not see any issues (compared to 11% in the USA and 12.6% in Germany).

Sharma et al. [30] conducted a survey from July 13, 2020, to August 13 with 261 participants from 27 countries. While having similar motivations, they found differences in the willingness to share personal information and with whom between the "Global North" and the "Global South," e.g., people from the North reported more often discomfort about sharing tracing data with large corporations.

Political Debates Häring et al. [16] asked for the participants' preferred political party and hypothesized that this could affect the willingness to install the German contact tracing app. The results do not indicate the preferred political party to be a factor; however, trust toward the government significantly influenced whether participants indicated they would use the app. Utz et al. [37] found something

[1] "The government's central scientific institution in the field of biomedicine"[34].

similar: A favorable rating of the state government and health authorities had a significant positive effect on the decision of whether the participants wanted to use an app. An unfavorable rating of the federal government had a negative influence.

For topics that are highly discussed in politics and where political stakeholderrs influence the outcome, it might thus be necessary to both ask participants about their general rating of these stakeholders, but also to understand and discuss the political and the societal situation in the country at the time of the study.

4.3 Privacy Concerns != Privacy Concerns

The literature shows that for many research questions, it is essential to know the participants' understanding of different concepts. Privacy concerns are likely based on participants' mental model of how things work, but that does not mean that the technical model actually has these problems; worse, it may even already mitigate the issues. Additionally, participants can have different understandings of what exactly would be privacy-invasive.

As an example of the latter, Häring et al. [16] reported that around 27% had concerns about their privacy in general. At the same time, many (around 58%) assumed that the app shows infected persons in the vicinity. It seems that many of the participants did not see this to be a problem for their privacy.

Utz et al. [37] asked for general negative aspects of contact tracing apps and also wanted to know why the participants did not use such an app at the time of the survey. Both questions were open-ended. While 40% of the German participants had privacy concerns in general, only around 10.5% mentioned privacy to be the reason why they currently use no such app. However, the unavailability of an app and the app being unnecessary were mentioned by 31% and 23% of the participants. It has to be noted that the official German app was released shortly after the survey. So while privacy concerns exist in general, this does not necessarily mean those privacy concerns also impact the rating of one specific app.

Lu et al. [21] further point out that in the context of contact tracing, there is a difference between informational privacy (e.g., control over personal information), social privacy (e.g., impression management), and interactional privacy (e.g., control of who to interact with). This might lead to seemingly inconsistent results: While participants, for example, mentioned that digital contact tracing would allow for anonymity, they were, at the same time, more willing to share data with a human contact tracer.

While the studies use privacy as a concept the way they ask about it is not always clearly defined. Two studies that used standardized approached were from Utz et al. [37] and Xie et al./Trestian et al. [35, 36, 39]. Utz et al. [37] used the IUIPC (2004) and found that, maybe counterintuitively, participants from China with higher privacy concerns (IUIPC: Control and Awareness) were more likely to use corona apps (not only tracing apps, but also apps with the purpose of symptom checks or quarantine enforcement). Xie et al. [39] found that, for Irish participants, the group of privacy fundamentalists (according to the PSI) was linked to the lowest adoption rate.

These are not per se contradicting results. One possible reason for that is that while the PSI and IUIPC have a similar goal, they cover slightly different aspects. The PSI concerns general privacy concerns, while the IUIPC focuses on online privacy. Also, both studies are conducted in different countries. Although the studies were conducted at similar times, the local situation may have influenced the results, e.g., Xie et al. report that the participants of their study report a change in their privacy concerns during the pandemic.

These different studies highlight again that it is crucial to be specific when talking about and conducting privacy research. For some of the studies, it is not clear what participants understood under the umbrella of "privacy." They provide valuable insights, but the different, sometimes unspecified, notions of privacy are hard to link to standardized tests, such as the IUIPC.

5 Conclusion

This chapter looked at contact tracing apps designed to combat COVID-19 and gave a brief overview of used techniques. Several studies looked at how the population perceived the aspect of privacy and how privacy concerns impacted the intention to install a contact tracing app. Summarized, it can be said that the public discussion was not completely detached from users as studies indeed reported privacy concerns, some of which are well-founded. Other concerns, however, cannot be traced back to actual technology. One example of this is the belief that the government has access to the data, even if the app followed a decentralized approach. Privacy concerns (in general or related to the app) were often associated with a lower willingness to install and use a CTA. However, when participants had the feeling that the app is unnecessary, they would also not install the app, even without privacy concerns. Another aspect of privacy research in the contact tracing context were methodological aspects that might have an influence on the results, such as the timing of the study, the context (e.g., political discussions), and the recruitment of participants. While the topic of contact tracing apps may vanish from the public radar as the need shrinks, there are still open research questions. It is still unclear whether and how the insights and opinions of the people shift over time. Additionally, it is to be seen if and how the findings can be applied to other areas as well, e.g., for enhanced monitoring of the spread of other diseases.

References

1. A flood of coronavirus apps are tracking us. Now it's time to keep track of them. Retrieved July 22, 2022, https://www.technologyreview.com/2020/05/07/1000961/launching-mittr-covid-tracing-tracker/
2. ACM Digital Library. Retrieved July 22, 2022, https://dl.acm.org/
3. Aji, Z. M., Mohd Salleh, N. S., Zakaria, N. H., & Mohd Khalid, A. H. (2021). Are you aware of your data privacy? The case of digital contact tracing applications (MySejahtera). In *2021 7th International Conference on Research and Innovation in Information Systems (ICRIIS)* (pp. 1–6).
4. Apple and Google partner on COVID-19 contact tracing technology. Retrieved 20, 2022, https://www.apple.com/newsroom/2020/04/apple-and-google-partner-on-covid-19-contact-tracing-technology/
5. Baumgärtner, L., Dmitrienko, A., Freisleben, B., Gruler, A., Höchst, J., Kühlberg, J., Mezini, M., Mitev, R., Miettinen, M., Muhamedagic, A., Nguyen, T. D., Penning, A., Pustelnik, D., Roos, F., Sadeghi, A.-R., Schwarz, M., & Uhl, C. (2020). 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)* (pp. 458–467).
6. Bundesregierung denkt bei App um. Retrieved July 22, 2022, https://www.tagesschau.de/inland/coronavirus-app-107.html
7. China launches coronavirus 'close contact detector' app. Retrieved July 22, 2022, https://www.bbc.com/news/technology-51439401
8. Contact tracing. Retrieved June 8, 2022, https://dictionary.cambridge.org/de/worterbuch/englisch/contact-tracing
9. Contact tracing in the European Union: Public health management of persons, including healthcare workers, who have had contact with COVID-19 cases—fourth update. Retrieved June 8, 2022, https://www.ecdc.europa.eu/en/covid-19-contact-tracing-public-health-management.
10. Contact Tracing Joint Statement. Retrieved July 22, 2022, https://www.esat.kuleuven.be/cosic/sites/contact-tracing-joint-statement/
11. Coronavirus disease (COVID-19): Contact tracing. Retrieved June 28, 2022, https://www.who.int/news-room/questions-and-answers/item/coronavirus-disease-covid-19-contact-tracing
12. COVID-19 and Your Health. Retrieved June 8, 2022 https://www.cdc.gov/coronavirus/2019-ncov/daily-life-coping/contact-tracing.html
13. Dooley, S., Turjeman, D., Dickerson, J. P., & Redmiles, E. M. (2020). 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. Association for Computing Machinery.
14. DP3T - Decentralized Privacy-Preserving Proximity Tracing. Retrieved July 22, 2022, https://github.com/DP-3T/documents
15. Eventregistrierung in der Corona-Warn-App. Retrieved July 22, 2022, https://www.bundesregierung.de/breg-de/themen/coronavirus/corona-warn-app-version-2-0-1889868
16. Häring, M., Gerlitz, E., Tiefenau, C., Smith, M., Wermke, D., Fahl, S., & Acar, Y. (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)* (pp. 77–98). USENIX Association.
17. Hinch, R., Probert, W., Nurtay, A., Kendall, M., Wymant, C., Hall, M., Lythgoe, K., Cruz, A. B., Zhao, L., Stewart, A., Ferretti, L., Parker, M., Meroueh, A., Mathias, B., Stevenson, S., Montero, D., Warren, J., Mather, N. K., Finkelstein, A., Bonsall, D., and Fraser, C. (2020). Effective configurations of a digital contact tracing app: A report to NHSX (p. 29).
18. Huang, Y., Obada-Obieh, B., Redmiles, E. M., Lokam, S., and Beznosov, K. (2022). 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 (pp. 12–24). Association for Computing Machinery.

19. IEEE Xplore. Retrieved July 22, 2022, https://ieeexplore.ieee.org/Xplore/home.jsp
20. Jamieson, J., Epstein, D. A., Chen, Y., & Yamashita, N. (2022). Unpacking intention and behavior: Explaining contact tracing app adoption and hesitancy in the United States. In *CHI Conference on Human Factors in Computing Systems*, CHI '22. Association for Computing Machinery.
21. Lu, X., L. Reynolds, T., Jo, E., Hong, H., Page, X., Chen, Y., & A. Epstein, D. (2021). 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. Association for Computing Machinery.
22. Mainzer Polizei nutzte Daten aus Luca-App ohne Rechtsgrundlage. Retrieved July 22, 2022, https://www.swr.de/swraktuell/rheinland-pfalz/mainz/polizei-ermittelt-ohne-rechtsgrundlage-mit-daten-aus-luca-app-100.html
23. Mozur, P., Zhong, R., and Krolik, A. (2020). In *Coronavirus fight, China gives citizens a color code, with red flags*. Retrieved September 26, 2022, https://www.nytimes.com/2020/03/01/business/china-coronavirus-surveillance.html
24. No, coronavirus apps don't need 60% adoption to be effective. Retrieved July 22, 2022, https://www.technologyreview.com/2020/06/05/1002775/covid-apps-effective-at-less-than-60-percent-download/
25. Open-Source-Projekt Corona-Warn-App – FAQ. Retrieved June 8, 2022, https://www.coronawarn.app
26. Pan-European Privacy-Preserving Proximity Tracing. Retrieved July 22, 2022, https://web.archive.org/web/20200409221119/https://www.pepp-pt.org/
27. Publicly-available Exposure Notifications apps. Retrieved July 29, 2022, https://developers.google.com/android/exposure-notifications/apps
28. Redmiles, E. M. (2020). User concerns & tradeoffs in technology-facilitated COVID-19 response. *Digital Government: Research and Practice, 2*(1), 1–12.
29. Shahroz, M., Ahmad, F., Younis, M. S., Ahmad, N., Boulos, M. N. K., Vinuesa, R., & Qadir, J. (2021). COVID-19 digital contact tracing applications and techniques: A review post initial deployments. *Transportation Engineering, 5*, 100072.
30. Sharma, T., Islam, M. M., Das, A., Haque, S. M. T., & Ahmed, S. I. (2021). Privacy during pandemic: A global view of privacy practices around COVID-19 apps. In *ACM SIGCAS Conference on Computing and Sustainable Societies*, COMPASS '21 (pp. 215–229). Association for Computing Machinery.
31. Sheeran, P. (2002). Intention–behavior relations: A conceptual and empirical review. *European Review of Social Psychology, 12*(1), 1–36.
32. Singapore reveals Covid privacy data available to police. Retrieved July 22, 2022, https://www.bbc.co.uk/news/world-asia-55541001
33. Speeding up detection to slow down Ebola: Smartphone app is game-changer for contact tracing in hotspots in the Democratic Republic of the Congo. Retrieved July 22, 2022, https://www.afro.who.int/news/speeding-detection-slow-down-ebola-smartphone-app-game-changer-contact-tracing-hotspots
34. The Robert Koch Institute. Retrieved July 22, 2022, https://www.rki.de/
35. Trestian, R., Celeste, E., Xie, G., Lohar, P., Bendechache, M., Brennan, R., & Ta, I. (2022). The privacy paradox—investigating people's attitude towards privacy in a time of COVID-19. In *2022 14th International Conference on Communications (COMM)* (pp. 1–6).
36. Trestian, R., Xie, G., Lohar, P., Celeste, E., Bendechache, M., Brennan, R., & Tal, I. (2021). PRIVATT—a closer look at people's data privacy attitudes in times of COVID-19. In *2021 IEEE International Mediterranean Conference on Communications and Networking (MeditCom)* (pp. 174–179).
37. Utz, C., Becker, S., Schnitzler, T., Farke, F. M., Herbert, F., Schaewitz, L., Degeling, M., & Dürmuth, M. (2021). Apps against the spread: Privacy implications and user acceptance of COVID-19-Related smartphone apps on three continents. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*, CHI '21. Association for Computing Machinery.

38. Web of Science. Retrieved July 22, 2022, https://www.webofscience.com/
39. Xie, G., Lohar, P., Florea, C., Bendechache, M., Trestian, R., Brennan, R., Connolly, R., & Tal, I. (2021). Privacy in times of COVID-19: A pilot study in the republic of Ireland. In *The 16th International Conference on Availability, Reliability and Security*, ARES 2021. Association for Computing Machinery.
40. Zampedri, G. (2021). To download, or not to download, that is the question: Investigating Belgian residents' motivation to download or not download the COVID-19 contact-tracing app Coronalert. In *2021 14th CMI International Conference—Critical ICT Infrastructures and Platforms (CMI)* (pp. 1–5).